iziar

e-magazine

50 Editions of IZIAR!

Answers To Actions:
The Era Of
AI

IPCS Global:
Empowering Skills, Inspiring Futures



Issue 50
November 2026

50Th Special Edition

The Technologies
Building Our Digital Future

About Us.

IPCS Global began its journey in 2008 with a vision to bridge the gap between education and industry. Over the past 18 years, from our first office in Kochi and training centre in Calicut, we have grown into a global network with a presence across India, Qatar, UAE, and Saudi Arabia.

As we celebrate the 50th edition of IZIAR, we reflect on a journey of learning, innovation, and continuous progress. We remain committed to empowering individuals with practical knowledge, industry-relevant skills, and opportunities for professional growth, while preparing them for the technologies and opportunities of tomorrow.



Our Top Trending Courses :

- Industrial Automation
- BMS & CCTV
- AI - Digital Marketing
- Python & Data Science
- Embedded & IoT
- Artificial Intelligence
- Cybersecurity and Ethical Hacking

Our Key Highlights :

- 100% Live & Interactive Sessions
- Government & Internationally Recognized Certifications
- Comprehensive Placement Support

Cooperation partner of TÜV SÜD

N·S·D·C National Skill Development Corporation

TABLE OF CONTENTS

01. Director's Desk: Connecting the Legacy with theTechnologies of Tomorrow.

04. Director's Desk: A Journey of Purpose Progress & Possibilities

06. Achieving Milestones Strength of Collective Effort

08. Celebrating 50 Editions, IPCS Global: Empowering Skills, Inspiring Futures

11. Your Resume Opens the Door, but Who You Are Makes the Difference The Little Things That Make a Big Difference

15. Classroom to Career: Bridging Talent, Technology & Opportunity

21. Beyond the Breakdown: Managing PLC Obsolescence and Migration

27. building Smarter Firmware: Bare Metal, FreeRTOS, and Zephyr Explained

35. Intelligent Maintenance: Fault Detection to Failure Prediction

TABLE OF CONTENTS

43. Code, Connect, Create: The Future of Full Stack Development

50. Answers to Action: The Next Era of AI

57. When Quantum Computing Challenges Cybersecurity

65. From Hijacking to Account Takeover: Defending the Digital Identity

71. Beyond SEO: How AEO Is Reshaping the Future of Google Search

77. Zero-Day Attacks: When Cybercriminals Strike Before Defenders Can Respond

84. Winning Attention without Losing Trust: The Human Equation in Digital Marketing

92. The Future of BMS: Autonomous and Smart Buildings

100. The Next Click: Redefining Digital Marketing

106. The Technologies Building Our Digital Future

115. Fifty Editions, One Vision: Celebrating the Journey of Iziar

Connecting the Legacy with the Technologies of Tomorrow...



UBAIDULLA MEKKUTH
DIRECTOR, IPCS GLOBAL

Fifty editions of a magazine reflect an organisation's initiative, commitment to continuous improvement, and dedication to sharing knowledge. As IPCS Global celebrates the 50th edition of IZIAR magazine, we take pride in this milestone and the opportunity it creates to connect our history with the technological developments shaping the future. In a rapidly changing world, sharing relevant knowledge is essential to helping students, professionals, and industry enthusiasts understand emerging opportunities.

Since IPCS began its journey in 2008 as an industrial automation service provider, technology has transformed significantly. From advances in automation to the growing influence of artificial intelligence, robotics, the Internet of Things, and data analytics, industries continue to evolve. These developments are changing how businesses operate and creating new possibilities across professional fields.



Understanding these technologies is important for students preparing for their careers and professionals looking to expand their knowledge. Beyond learning about new tools, it is equally important to understand their practical applications and how they address real-world challenges. IZIAR can help bridge this gap by presenting emerging developments in an accessible and engaging way.

As technology continues to advance, continuous learning and adaptability become increasingly valuable. Existing skills must evolve alongside industry requirements, while curiosity and critical thinking help individuals explore unfamiliar areas. For businesses and professionals alike, staying informed about technological developments can open new perspectives and help them prepare for future opportunities.

Technology also connects fields that were once considered separate. Industrial automation now intersects with software, data analysis, and intelligent systems, demonstrating how different disciplines contribute to modern industry. Understanding these connections helps readers develop a broader view of technology and its practical impact. For IPCS Global, our history has unfolded alongside significant changes in automation, engineering, and digital technology. IZIAR complements this journey by providing a platform to share knowledge, explore new ideas, and keep readers informed about developments that matter. The 50th edition is not just a publishing milestone; it is an opportunity to reaffirm the importance of knowledge-sharing in a world that never stops evolving.



As we look ahead, I hope IZIAR will continue to inspire students, support professionals, and encourage readers to explore emerging technologies with curiosity and confidence. By making knowledge accessible and relevant, the magazine can help readers better understand the present and prepare for the possibilities of tomorrow.

On this special occasion, I extend my heartfelt congratulations to the entire IZIAR team and everyone who has contributed to this journey. My sincere appreciation goes to our students, professionals, readers, and well-wishers whose participation and support have made this milestone meaningful. May the 50th edition inspire many more years of learning, innovation, and knowledge-sharing. Here's to celebrating our legacy, embracing technological change, and creating new possibilities for the future.



A Journey of Purpose

Progress & Possibilities



JAMAL NADAKKAVIL
DIRECTOR, IPCS GLOBAL

Reaching the 50th edition of IZIAR is a proud milestone for IPCS Global. It represents more than the continuation of a publication; it reflects our journey of learning, growth, shared experiences, and the collective commitment of everyone who has been part of our organisation. Since our beginnings in 2008, IPCS has continued to evolve with a clear purpose: to bridge the gap between education and industry by equipping individuals with relevant skills, practical knowledge, and the confidence to pursue meaningful careers. What began with a foundation in industrial automation has grown into a broader learning ecosystem that addresses the changing needs of technology, industry, and employment.

The journey has reinforced an important belief: education creates its greatest impact when knowledge is translated into practical ability. As industries evolve and new technologies reshape the professional landscape, the responsibility of a training institution extends beyond delivering lessons. It must prepare learners to adapt, think critically, solve problems, and remain committed to continuous development. At IPCS Global, we recognise that this responsibility requires constant improvement.



Our focus on practical training, industry-relevant learning, expert guidance, and placement assistance reflects our commitment to helping students move forward with greater clarity and confidence. Every learner who enters our institution brings a unique ambition, and supporting that ambition remains central to our work.

However, an organisation's growth is never the achievement of one individual. It is the result of dedicated teams, committed trainers, supportive parents, industry partners, and students who trust the journey. Their contributions have helped shape IPCS Global into the organisation it is today. I extend my sincere gratitude to everyone who has contributed to this progress. As we celebrate this 50th edition of IZIAR, I also recognise the value of communication and shared knowledge. A magazine provides an opportunity to document achievements, highlight ideas, celebrate people, and strengthen the connection we share as an organisation. IZIAR serves as a reflection of our journey and a record of the people and experiences that continue to shape it.



Looking ahead, our ambition is to keep moving forward with purpose. We will continue to explore emerging technologies, strengthen industry connections, improve learning experiences, and expand opportunities for aspiring professionals. Growth, for us, is not simply about reaching new milestones; it is about creating lasting value for learners, industry, and society. To our students, I encourage you to remain curious, embrace challenges, and never stop learning. To our team, thank you for your dedication and commitment. And to everyone who has placed their trust in IPCS Global, thank you for being part of this journey. The 50th edition is a moment to reflect on how far we have come and to renew our commitment to what lies ahead. May IZIAR continue to share our stories, inspire new ideas, and celebrate the people who make our journey meaningful. With gratitude for the journey so far and confidence in the possibilities ahead.



Strength of Collective Effort



AJITH SURENDRAN
GENERAL MANAGER, IPCS GLOBAL

Every milestone an organisation achieves reflects the dedication of its people, the strength of its shared vision, and the commitment to keep moving forward. As IPCS Global celebrates the 50th edition of IZIAR, we have an opportunity to reflect on the efforts, collaboration, and shared purpose that continue to shape our journey. This milestone is not just a measure of how far we have come, but also a reminder of the people whose contributions make every step forward possible. In an organisation focused on education and professional development, progress is measured by more than the number of programmes delivered or milestones achieved. It is also reflected in the quality of learning, the confidence students develop, the skills they acquire, and the opportunities they are prepared to pursue. These outcomes require commitment at every level of the organisation.

At IPCS Global, our work involves bringing together students, trainers, academic teams, placement professionals, and industry partners. Each plays an important role in creating a learning environment that supports both professional and personal development. When these efforts work together, they help transform the student experience from classroom learning into practical preparation for the workplace. One of our key priorities is ensuring that training remains relevant to the needs of industry.

Technology and job requirements continue to evolve, making practical exposure, problem-solving abilities, and adaptability increasingly important. Our focus on hands-on learning, real-time projects, expert mentoring, and placement assistance reflects the need to prepare students for the expectations they may encounter in their professional journeys.



Achieving this requires continuous coordination and a willingness to improve. From maintaining training standards to supporting students throughout their learning journey, every process matters. We must regularly evaluate our methods, respond to feedback, and identify opportunities to make our systems more effective. Sustainable growth comes from consistently doing the fundamentals well while remaining open to change. I would also like to acknowledge the contribution of our team members across different departments and branches.

Their daily efforts, often behind the scenes, help maintain the standards and services that students and families expect from us. Every successful programme, positive student experience, and organisational achievement is supported by the collective work of many individuals. Their commitment deserves recognition and appreciation.

Our students are equally important to this journey. Their aspirations remind us why our work matters. Each student arrives with different goals, abilities, and challenges. Providing the right guidance, encouraging independent thinking, and helping learners recognise their potential are responsibilities we must continue to take seriously. The progress of our students remains one of the most meaningful indicators of our work. The 50th edition of IZIAR is also a reminder of the importance of documenting our progress and learning from our experiences. It gives us a platform to acknowledge achievements, share perspectives, and strengthen the sense of connection across the IPCS Global community. I congratulate everyone who has contributed to bringing this edition to life.



As we move forward, our focus remains on strengthening our processes, improving the learning experience, supporting our teams, and building stronger connections with industry. The opportunities ahead will require flexibility, collaboration, and a shared commitment to excellence. I believe the next phase of our journey will be shaped by the quality of our teamwork and our ability to turn plans into meaningful outcomes. Every improvement matters, every contribution counts, and every student deserves our best efforts.

Congratulations to the entire IPCS Global family on this significant milestone. May the journey ahead bring continued learning, stronger collaboration, and progress that we can all take pride in. Our vision sets the direction, but it is our collective effort that moves us forward.



50 Editions



RAKESH K C
TECHNICAL HEAD, IPCS GLOBAL

IPCS Global: Empowering **Skills, Inspiring Futures**

Every milestone tells a story of dedication, growth, and progress. The publication of the 50th edition of IZair Magazine marks a proud moment in our journey—a celebration of knowledge, innovation, learning, and the opportunities that shape tomorrow. This achievement reflects our continued commitment to sharing ideas, inspiring minds, and highlighting the transformative power of skills in an ever-changing world.

As we celebrate this special edition, we are reminded that the future belongs to those who are willing to learn, adapt, innovate, and grow. In today's rapidly evolving professional landscape, academic qualifications alone are no longer enough. Industries seek individuals who combine technical knowledge with practical expertise, problem-solving abilities, creativity, and the confidence to turn ideas into real-world solutions.

At IPCS Global, our mission has always been to bridge the gap between education and industry by transforming learners into skilled, confident, and industry-ready professionals. Every student trained, every skill developed, and every career opportunity created represents a step towards building a more capable and future-ready workforce.

Through specialized training in Industrial Automation, Embedded Systems and IoT, Building Management Systems (BMS), Full Stack Development, Data Science and Artificial Intelligence, Information Technology, and Digital Marketing, we emphasize hands-on learning, practical experience, and industry-relevant technologies. Our approach goes beyond theoretical instruction, empowering learners to apply their knowledge, solve practical challenges, and confidently pursue their professional ambitions.







One of the key challenges facing today's workforce is the gap between academic learning and industry expectations. Employers need professionals who can translate knowledge into action, adapt to changing technologies, and contribute effectively in real-world environments.

Through experiential learning, technical competency development, and industry-focused training, IPCS Global strives to prepare learners for these expectations and strengthen their employability.

Our commitment to industry readiness is further strengthened through corporate engagement, industry collaborations, and placement-oriented initiatives. By connecting skilled learners with potential employers, we help create pathways to meaningful careers while supporting organizations in finding the talent they need to grow and innovate.As technology continues to reshape industries, the importance of continuous learning has never been greater. Artificial Intelligence, automation, connected systems, and digital transformation are opening new possibilities while redefining the skills required for tomorrow's workforce. In this environment, the willingness to learn, evolve, and embrace change remains one of the most valuable assets a professional can possess.

Reaching the 50th edition of Izair Magazine is more than a publishing milestone—it is a celebration of the power of ideas, the value of knowledge, and the possibilities created through continuous learning. It represents an ongoing journey of sharing insights, encouraging innovation, and bringing together perspectives from education, technology, and industry. This special edition also serves as a reminder that every meaningful achievement begins with curiosity and grows through commitment and collaboration.

As we celebrate this remarkable milestone, IPCS Global renews its commitment to empowering individuals with practical skills, nurturing industry-ready talent, and creating opportunities for professional growth. Looking ahead, we remain focused on embracing emerging technologies, strengthening industry connections, and helping learners prepare for the challenges and opportunities of a rapidly transforming world.

The journey of 50 editions is a moment to celebrate how far we have come—and an inspiration to explore how much further we can go. With every new idea, every skill acquired, and every opportunity created, we move closer to a future driven by knowledge, innovation, and human potential.

The future belongs to those who transform knowledge into action, skills into opportunities, and ambition into achievement.





REKHA PRAMPARAMBATH
HR Manager , IPCS GLOBAL

Your Resume Opens the Door, But Who You Are Makes the Difference

The Little Things That Make a Big Difference



A reflection from an **HR Manager's desk** The interview room was ready. A few resumes lay neatly on the table. Outside, a group of young graduates waited for their turn, each carrying a dream, a little nervousness, and the hope of beginning a new chapter in life. One by one, they walked into the room. Each had a different story, a different background, and a different idea of success. As an HR Manager, I often meet young people at this important turning point in their lives. Some arrive with impressive academic achievements. Some have completed exciting projects. Others are still discovering what they are truly good at. Yet, every candidate reminds me of one simple truth: behind every resume is a person with a story waiting to be discovered. And that is where the real journey begins.

More Than a Piece of Paper

A resume is a wonderful introduction. It tells us what you have studied, the skills you have developed, and the experiences you have gained. But a resume can only tell part of your story. It cannot fully show the curiosity that makes you ask one more question, the kindness that makes you help a teammate, or the determination that keeps you going when something feels difficult. These qualities often reveal themselves in the smallest moments. A student who takes responsibility for a college event learns leadership. Someone who explains an idea during a group discussion develops communication skills.

A student who tries a new project discovers the confidence to explore unfamiliar things. You may not always recognize these moments as career preparation, but they are quietly shaping the professional you will become. Sometimes, the most valuable lines on your future resume begin with experiences you never thought were important.



The Question Behind
The Questions

During an interview, students often prepare for one familiar question: "Tell me about yourself." They think about their degree, their marks, their strengths, and their achievements. These are all important. But an interview is also an opportunity to share how they think, what they have learned, and what they hope to contribute. When I ask a candidate about a college project, I am interested in more than the final result. I want to understand the journey. How did they approach the task? How did they work with others? What did they discover along the way? There is no need for a dramatic success story. Even a small experience can reveal something meaningful when you speak about it honestly. So, dear students, do not wait until you have a big achievement to talk about. Learn to recognize the value of your everyday experiences. You may discover that you have more to share than you realize.

Skills Are Built in
Ordinary Moments

We sometimes imagine that professional skills are developed only through special courses or formal training. In reality, many of them begin in ordinary college life. When you listen carefully to a classmate, you practise communication. When you divide responsibilities during a group assignment, you learn teamwork. When you organize a programme, you practise planning and leadership. When you look for a solution instead of giving up on a difficult task, you develop problem-solving skills. These experiences may seem small today, but they prepare you for situations you will encounter in the workplace. The good news is that you do not need to wait for your first job to start becoming job-ready. Your classroom can be your first workplace. Your projects can be your first professional experiences. And every new challenge can become a lesson in growth.



A World That Never Stops Learning

The workplace you enter today may look very different from the one your seniors entered a few years ago. Artificial intelligence, digital tools, and new technologies are changing how people work and how businesses grow. This change brings exciting possibilities for young professionals. You do not need to master every new tool or know everything about your industry before graduation. Start with curiosity. Explore technology that is relevant to your field. Learn how to use AI responsibly. Ask questions, test ideas, and keep updating your knowledge. Along with technical skills, continue developing qualities that help you make good decisions: creativity, clear thinking, empathy, and the ability to work with people. Technology can help you do many things, but your willingness to learn how to use it wisely is what turns it into an advantage. The future belongs to those who are ready to grow with it, one step at a time.

Confidence Does Not Always Make Noise

When we think of confidence, we often imagine someone who speaks boldly, answers every question quickly, and walks into a room without hesitation. But confidence can be quiet, too. It is the courage to ask a question when you do not understand something. It is the willingness to share an idea even when you feel nervous. It is the honesty to say, "I don't know yet, but I am willing to learn." You do not have to become someone else to succeed. You do not need to be the loudest person in the room or the person with the longest list of achievements. Learn to recognize your strengths. Work on the areas where you want to improve. Give yourself opportunities to practise. With time, small efforts build genuine confidence. As an HR Manager, I believe that a young person who is sincere, open to feedback, and eager to improve has a wonderful foundation on which to build a career.



There is something special about a first job. It is the moment when the lessons learned in classrooms begin to connect with the realities of professional life. You will meet new people, face unfamiliar situations, discover new responsibilities, and learn things that no textbook could teach you in quite the same way. Give yourself permission to be a beginner. Ask for guidance. Learn from your colleagues. Accept feedback with an open mind. Celebrate your progress, even when it comes in small steps. Every experience adds another layer to your understanding of yourself and the world around you. Your first job does not require you to have a perfect story. It gives you the opportunity to begin writing one. And that, perhaps, is one of the most beautiful things about starting a career: there is still so much to discover.



Your First Job Is the Beginning, Not the Destination

Dear students, as you prepare to enter the professional world, I hope you look at your future with excitement rather than fear. Keep your academic knowledge strong. Build practical skills. Learn to communicate with kindness and clarity. Stay curious about technology. Treat people with respect. Take opportunities that help you grow, even when they seem small. Most importantly, do not measure your potential only by the opportunities you have received so far. There is so much you can still learn, create, and achieve. When your resume is placed on an interviewer's desk, let it be the beginning of a wonderful conversation about the person you are becoming. Because beyond your qualifications lies your character. Beyond your skills lies your willingness to learn. And beyond your first job lies a future full of possibilities. Your resume may open a door, but your curiosity, character, and commitment to growth will help you make the most of what lies beyond it. So, keep learning. Keep exploring. Keep becoming. Your story has only just begun. With warm wishes for your journey ahead,

Classroom to Career:
Bridging Talent, Technology & Opportunity



GIFTY KP
Zonal Manager(Placements)
IPCS GLOBAL

Celebrating 50 Editions of IZIAR: A Journey of Shared Growth

There is something special about a first job. It is the moment when the lessons learned in classrooms begin to connect with the realities of professional life. You will meet new people, face unfamiliar situations, discover new responsibilities, and learn things that no textbook could teach you in quite the same way. Give yourself permission to be a beginner. Ask for guidance. Learn from your colleagues. Accept feedback with an open mind. Celebrate your progress, even when it comes in small steps. Every experience adds another layer to your understanding of yourself and the world around you. Your first job does not require you to have a perfect story. It gives you the opportunity to begin writing one. And that, perhaps, is one of the most beautiful things about starting a career: there is still so much to discover.



For me, this question has been central to my professional journey. Working in the Education Technology (EdTech) industry has shown me that education creates its greatest impact when learning extends beyond the classroom and opens doors to real-world opportunities.

A Journey Shaped by Learning and Purpose

With over 10 years of experience in the EdTech industry, I have witnessed considerable changes in the way education is delivered, skills are developed and employment opportunities are created. The expectations of both learners and employers have evolved, making practical knowledge, adaptability and professional readiness increasingly important.

A qualification provides a foundation, but students also need the confidence and ability to apply what they have learned. Similarly, employers need professionals who understand workplace expectations and can contribute effectively from the beginning of their careers.

These experiences have shaped my approach to placement management. I see placement as much more than sharing vacancies or arranging interviews. It involves preparing students, understanding employer requirements,

building professional relationships and creating a process through which the right opportunities reach the right candidates.

When education and industry work together, students gain a clearer understanding of their future, and employers gain access to talent that is better prepared for the workplace.

My Journey with IPCS Global: Turning Opportunities into Outcomes

My journey with IPCS Global over the past two-plus years has been an important chapter in my professional life. As Zonal Manager – Placements, I oversee placement activities across the South and North Zones, working towards a common goal of strengthening industry connections and expanding career opportunities for students.

The role brings together several responsibilities, including developing corporate relationships, coordinating recruitment drives, guiding placement teams, improving branch-level processes, analyzing performance and ensuring that placement activities reflect both student aspirations and industry expectations.

One of the most valuable aspects of this work has been expanding our corporate network, which now includes more than 3,000 company connections.

Each connection creates the possibility of a recruitment opportunity, industry collaboration, a hiring partnership or a better understanding of the skills employers are looking for.

However, building a strong placement ecosystem requires more than maintaining a list of companies. It depends on regular communication, consistent follow-up, an understanding of changing recruitment needs andrelationships built on trust.

At IPCS Global, I have also worked towards strengthening a more structured and student-focused placement culture. This includes improving placement readiness, encouraging greater participation in recruitment drives, enhancing communication between branches and the placement team, and aligning activities with measurable outcomes. Ultimately, the goal is to help students approach the employment process with the right preparation, relevant skills and confidence in their abilities.

Understanding the Changing World of Employment

The employment landscape is evolving rapidly. Artificial intelligence, automation and digital transformation are changing the way organizations operate, recruit and evaluate talent. As a result, employers are increasingly looking beyond academic qualifications to assess practical abilities, adaptability and the willingness to learn.

Several developments are shaping the future of recruitment and career preparation:

AI-powered recruitment: Technology is increasingly supporting candidate screening, recruitment processes and career preparation.

Skills-based hiring: Practical competence and demonstrable skills are becoming increasingly importantalongside formal qualifications.

Continuous learning: Professionals need to keep updating their knowledge as technologies and workplace requirements change.

Industry–academia collaboration: Stronger connections between educational institutions and employers can help align training with real industry needs.

Digital career platforms: Online platforms are creating new ways for students to discover opportunities, access resources and stay informed about recruitment activities.

These changes reinforce an important belief: education must remain connected to the realities of the workplace. Institutions that bring together knowledge, practical skills, technology and employment will be better positioned to prepare students for a changing professional world.



Talenzo: An Idea Built Around Student Needs

TALENZO
Connecting Talent with Opportunity

One of the most meaningful initiatives in my journey at IPCS Global has been Talenzo, the student placement website I conceptualized and created.

The idea began with a simple, practical question: How can students access placement opportunities and learning resources more easily, without having to depend on scattered updates and communication channels?

When placement information and study materials are shared through different channels, students may find it difficult to keep track of updates or locate the information they need. A dedicated digital platform offered an opportunity to make this process more organized and accessible.

Talenzo was developed with the vision of bringing placement information, student access and learning resources together in one digital environment.

The platform is designed to support several important functions:

Centralised vacancy updates: Providing students with a dedicated space to access placement opportunities.

Student portal access: Allowing students to log in, manage their profiles and maintain relevantinformation.

Learning resource sharing: Making study materials and placement-related resources available through a common platform.

Improved communication: Creating a more organized channel for sharing important placement updates.

Scope for future development: Establishing a digital foundation that can evolve according to student feedback and organizational needs.



What makes Talenzo particularly meaningful to me is the process of turning an idea into a practical solution. Developing a digital platform alongside my placement responsibilities required planning, coordination, testing, problem-solving and a willingness to explore areas beyond my established professional experience. The journey also reinforced an important lesson: innovation does not always begin with a large team or complexinfrastructure. Sometimes, it starts with recognizing a recurring challenge, thinking differently about how to address it and taking the initiative to develop a solution.

For me, Talenzo represents an effort to make placement-related information more accessible and support a more organised experience for students. Its future development can build on user feedback and the evolving

Technology Matters, But People Matter More

As digital platforms and artificial intelligence become more prominent in education and recruitment, placement management will continue to change. Technology can organize information, simplify processes and support decision-making, but it cannot replace the importance of human understanding, communication and trust.

A digital platform may help identify a suitable candidate, but students may still need guidance to prepare for an interview. Recruitment data may highlight a skill gap, but individuals need the right support to address it.

Online tools may expand access to vacancies, but meaningful employers relationships help turn those vacancies into lasting opportunities.

This is where I believe the future of EdTech and placement management lies: using technology to make processes more efficient while keeping people at the centre of every decision. For placement teams, this means adopting useful digital solutions, understanding emerging technologies and developing strategies that reflect industry expectations.

For educational institutions, it means looking beyond course completion and considering practical competence, employability, employer feedback and the preparedness of students for the workplace. For students, it means recognizing that learning does not end with a certificate. It continues through practice, experience, curiosity and the ability to adapt to change.

Technology can make opportunities easier to find, but guidance, preparation and determination help students make the most of them.



Looking Ahead: Creating Impact through Collaboration

Looking back on my professional journey, one lesson continues to stand out: meaningful progress happens when knowledge is translated into action and people work together towards a shared purpose. My experience in EdTech has given me a broader understanding of education, skill development and the changing expectations of the employment market.

My journey at IPCS Global has strengthened my experience in placement leadership, corporate engagement, team development and operational management. Working on Talenzo has also allowed me to explore digital innovation and apply problem-solving to a practical need.

As I celebrate the 50th edition of IZIAR, I am reminded that progress is rarely the result of one effort alone. It grows through collaboration, continuous learning, shared ideas and the willingness to improve.
The future will bring new technologies, new job roles and new expectations. Preparing students for that future requires educational institutions, industry partners and placement professionals to work together, creating an environment in which learning leads to opportunity.

For me, the purpose remains clear: to help bridge the gap between what students learn and what the industry needs, while making opportunities more accessible through meaningful relationships and practical innovation.

Education builds potential. Industry opens doors. Technology brings them closer. And people make the connection meaningful.



Beyond the Breakdown: Managing PLC Obsolescence & Migration



IBENE BABU
Territory Technical Head,
IPCS GLOBAL KOCHI

Many industrial plants continue to operate PLC systems that were installed more than a decade ago. Although these controllers may still perform reliably, their supporting infrastructure can gradually become outdated. Manufacturers discontinue product families, engineering software loses support, spare parts become difficult to source, and experienced engineers move on. The problem often remains unnoticed until a critical controller fails. Maintenance teams may struggle to find replacement components, recover the latest program, or identify undocumented modifications. What should have been a routine repair can quickly become an expensive production interruption.

PLC obsolescence is therefore more than a hardware issue. It is a lifecycle management challenge that requires engineering, maintenance, procurement, and management to work together. The objective is not to replace every old controller immediately. It is to understand the risks, prepare for future failures, and plan migrations before production is affected.

Why Proactive Lifecycle Management Matters

Reactive maintenance begins when equipment fails. Proactive lifecycle management begins byidentifying what could fail, how serious the consequences would be, and what action is needed. A well-managed PLC fleet has an accurate asset register, verified program backups, a clear spare-parts strategy, and an assigned team responsible for monitoring equipment lifecycle status. These measures help reduce uncertainty and give the organisation time to make informed decisions.



Three strategies are commonly useful:

Sustain: Continue using a reliable platform while maintaining backups, suitable spares, and regular lifecycle reviews.

Bridge: Introduce carefully designed gateways or compatible systems to address immediate limitations while preparing for future migration.

Migrate: Replace the existing platform when support limitations, recurring failures, component availability, or operational risks justify the investment.

The right choice depends on the controller's condition, manufacturer support, system criticality, and the consequences of downtime

Six Areas Every Plant Should Assess

PLC obsolescence extends beyond the controller itself. Effective assessment should cover six areas:

Hardware: Controller models, revisions, I/O modules, and replacement availability

Software: Firmware, programming tools, HMI and SCADA versions, and compatibility.

Communication: Fieldbus networks, Industrial Ethernet, gateways, and connected devices

Spares: Inventory, storage condition, authenticity, and supplier lead times.

Criticality: Production impact, recovery time, quality risks, and safety implications.

Ownership: Documentation responsibility, lifecycle monitoring, and migration funding.

A relatively modern PLC with missing backups may create greater recovery difficulties than an older, well-documented controller with verified spares. This is why age alone should not determine migration priorities.

Building a Reliable PLC Inventory

The first practical step is to create an accurate record of the installed automation systems. Each PLC or control cell should have documented hardware details, firmware versions, engineering software, I/O configurations, wiring diagrams, communication settings, spare-parts availability, and manufacturer lifecycle information.

Program backups must be current, securely stored in more than one appropriate location, and restorable where practical. Records should also include HMI projects, drive parameters, network configurations, and relevant electrical drawings. A structured spreadsheet is sufficient to begin. The important requirement is that someone maintains it.Integrating the register with a Computerised Maintenance Management System (CMMS) can help ensure that hardware replacements and software changes trigger documentation updates.



Planning a Successful PLC Migration

A successful migration requires more than installing a new CPU and transferring the old program. It involves several carefully managed stages.

1. Discovery and assessment

Inspect the existing system, document its configuration, identify connected devices, and review operational behaviour. Record recurring alarms, communication issues, and process requirements. This establishes a baseline against which the new system can be evaluated.

2. Design and program conversion

Determine whether the existing logic can be converted, adapted, or must be rewritten. Differences in instructions, addressing, communication functions, and timing behaviour can prevent direct conversion.
Engineers should also define I/O mappings, testing requirements, and any necessary changes to the control architecture.

3. Bench testing and simulation

Where feasible, test the converted program using simulated I/O, a test bench, or a representative machine section. Verify automatic and manual modes, fault handling, recovery sequences, communication, alarms, and timing-sensitive operations. Simulation helps identify problems before the system reaches the production floor, but it does not replace physical commissioning.





4. Controlled cutover

For many existing plants, migrating one machine or production zone at a time is less risky than replacing the entire system in a single shutdown. Each stage should have defined acceptance criteria, assigned responsibilities, and a documented rollback procedure. Verified backups and clear stop-work conditions are essential.

5. Commissioning and handover

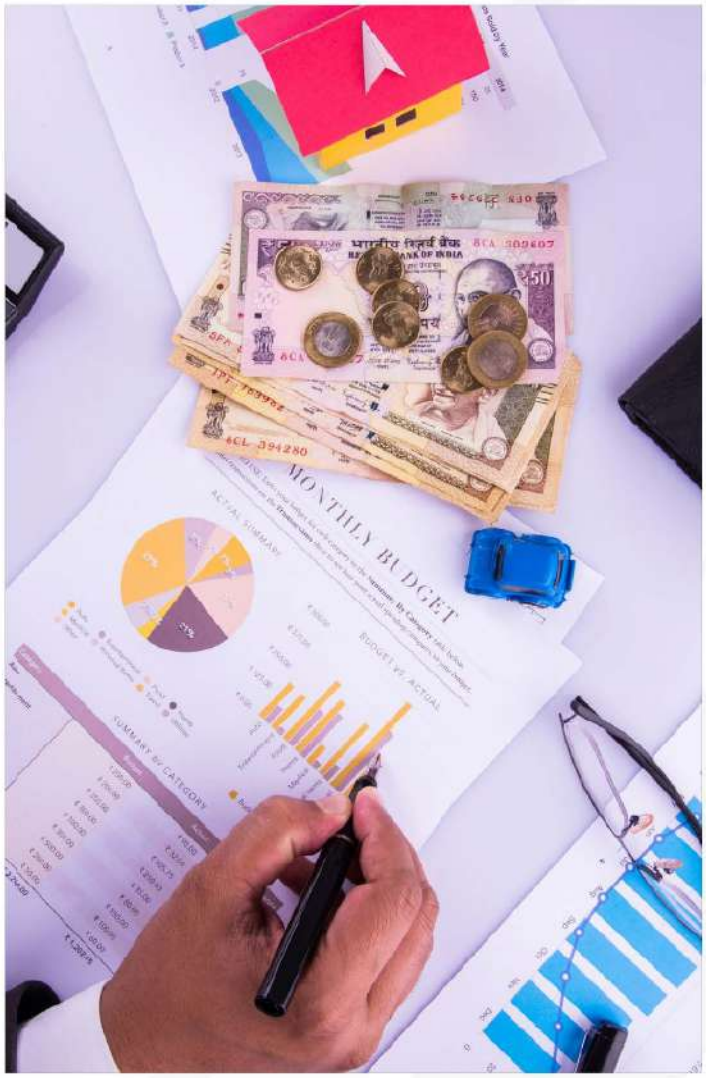
After cutover, monitor system performance, resolve emerging issues, and update the as-built drawings, network diagrams, I/O lists, software records, and maintenance instructions. Train relevant personnel and verify that the new system is properly documented and supportable. Safety-related functions require appropriate assessment and validation by qualified personnel throughout the process.

Practical Lessons From Industry

Consider an ageing conveyor system that cannot tolerate a lengthy shutdown. A phased migration allows engineers to modernise individual zones while maintaining the remaining system, provided the interfaces and changeover arrangements are carefully engineered. In another situation, a legacy PLC may still control the process reliably but lack convenient connectivity to modern SCADA or Manufacturing Execution Systems (MES). A suitable gateway may provide access to selected operational data while the original controller remains in service. Such connections must be designed with cybersecurity, access control, and communication reliability in mind.

Where immediate migration is not feasible, securing verified critical spares and improving documentation can reduce short-term risk. However, this should remain a managed temporary measure, not a substitute for long-term planning.

Ownership, Budgeting, and Business Benefits



Lifecycle management often fails because responsibility is unclear. Plants should assign a controls engineer or team to maintain the asset register, monitor manufacturer announcements, review spare availability, and identify systems requiring investment.

Budgets should account for critical spares, engineering effort, lifecycle monitoring, and planned migrations. Some organisations use 2–4% of installed automation asset value annually as an initial budgeting reference, but the appropriate allocation varies with equipment age, criticality, support status, and downtime costs.

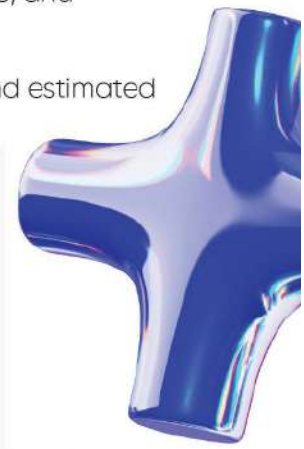
A proactive programme can reduce unplanned interruptions, improve cost control, preserve engineering knowledge, support safer migrations, and make capital expenditure more predictable.

A Practical 90-Day Action Plan

Plants can begin with five steps:

1. Select one critical production line and document its PLC hardware, software, communication architecture, and lifecycle status.
2. Collect and verify PLC, HMI, drive, and network backups.
3. Assess spare availability and classify each controller as sustain, bridge, or migrate.
4. Prepare a migration proposal for one high-priority system, including testing, downtime, and rollback requirements.
5. Present management with a three-year lifecycle roadmap covering priorities, risks, and estimated investment.

This approach turns a broad technical concern into an actionable engineering plan.

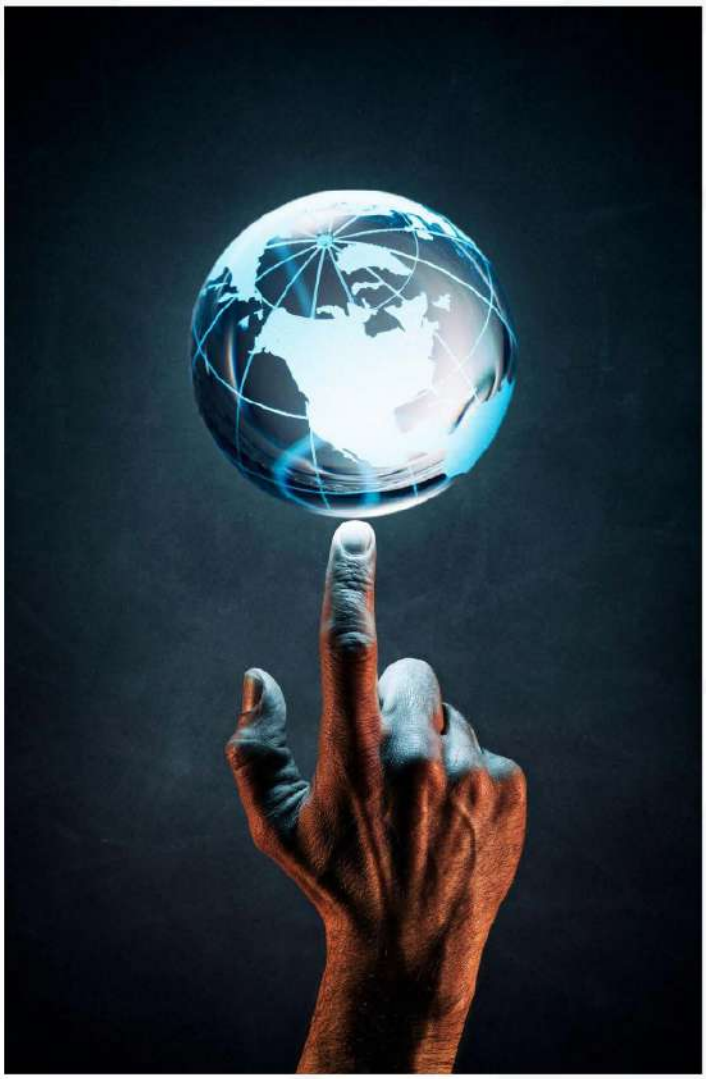


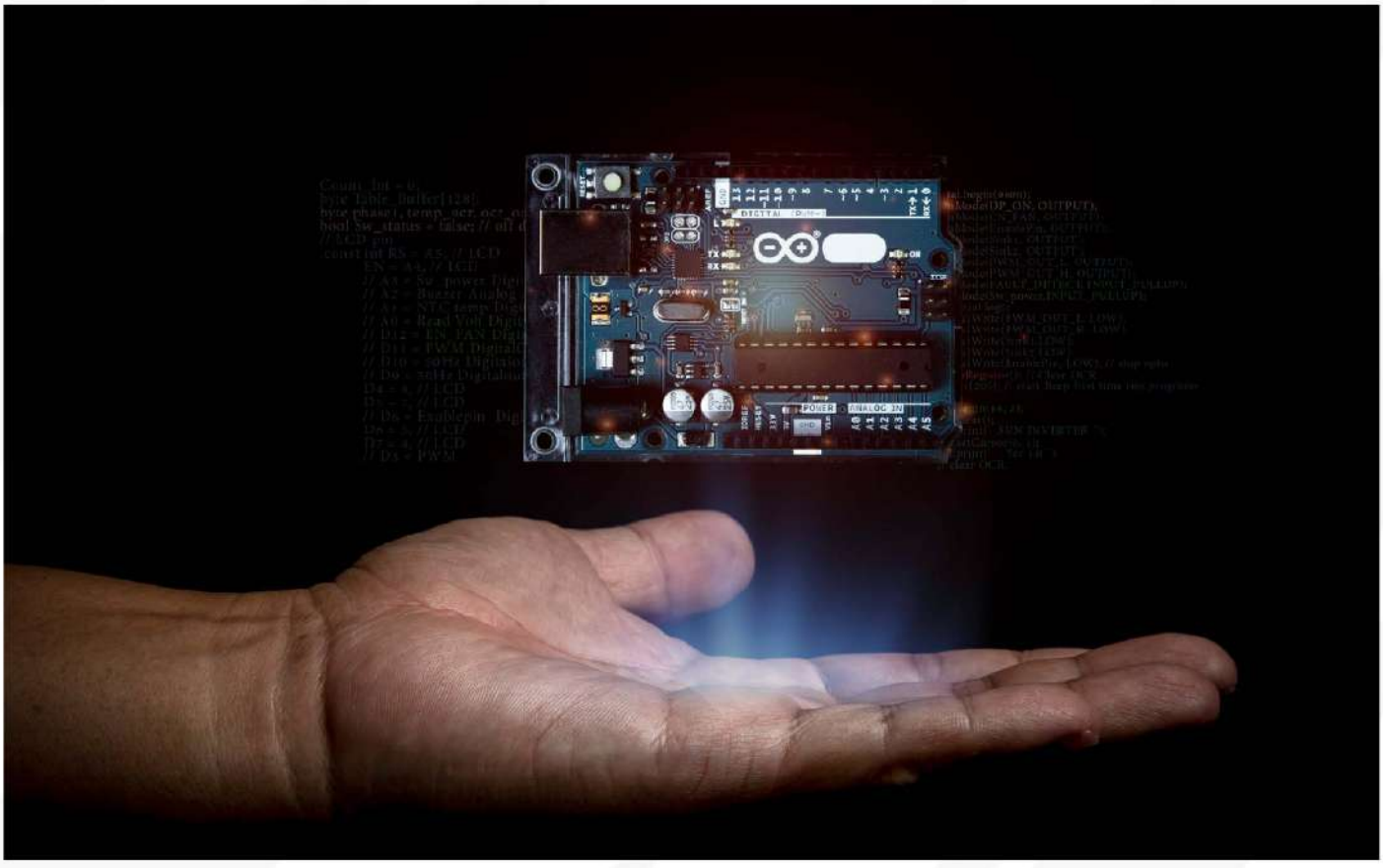
Preparing For The Future

As industries adopt Industry 5.0, connected manufacturing, advanced analytics, and AI-assisted operations, reliable automation infrastructure remains essential. New technologies cannot compensate for undocumented control systems, unavailable spare parts, or unusable backups.

The goal is not to eliminate every ageing PLC. It is to understand each system's condition, manage its risks, and plan the right intervention at the right time.

A reliable plant does not wait for a critical PLC to fail before planning its replacement. It recognises the warning signs, prepares its resources, and turns a potential emergency into a controlled engineering decision.





Building Smarter Firmware:

Bare Metal, FreeRTOS, & Zephyr Explained



FAREEDA
PROJECT ENGINEER,
IPCS GLOBAL CALICUT

Every embedded developer eventually faces an important design decision: should an application run directly on the hardware, or does it need a real-time operating system (RTOS)?
This decision influences firmware performance, memory usage, development time, debugging complexity, and future scalability. A simple temperature controller may work perfectly with bare-metal programming, while a connected industrial monitoring device may require an RTOS to manage sensors, communication, data processing, and user interfaces simultaneously.

Among the available approaches, bare-metal programming, FreeRTOS, and Zephyr offer different advantages. Understanding their strengths and limitations helps developers select the right architecture for their application.



Bare-Metal Programming: Simplicity and Control

Bare-metal programming allows software to execute directly on a microcontroller without an operating system. Developers typically write a main function containing an infinite loop, commonly called a super loop, that repeatedly reads inputs, processes information, and controls outputs.

For example, a basic embedded application might read a temperature sensor, process the measurement, and update a display. Interrupt service routines (ISRs) handle events that require immediate attention.

Advantages of Bare Metal

Low resource consumption: Without an operating system or scheduler, bare-metal applications can operate with minimal RAM and flash memory.

Direct hardware control: Developers have precise control over peripherals, interrupts, and execution sequences.

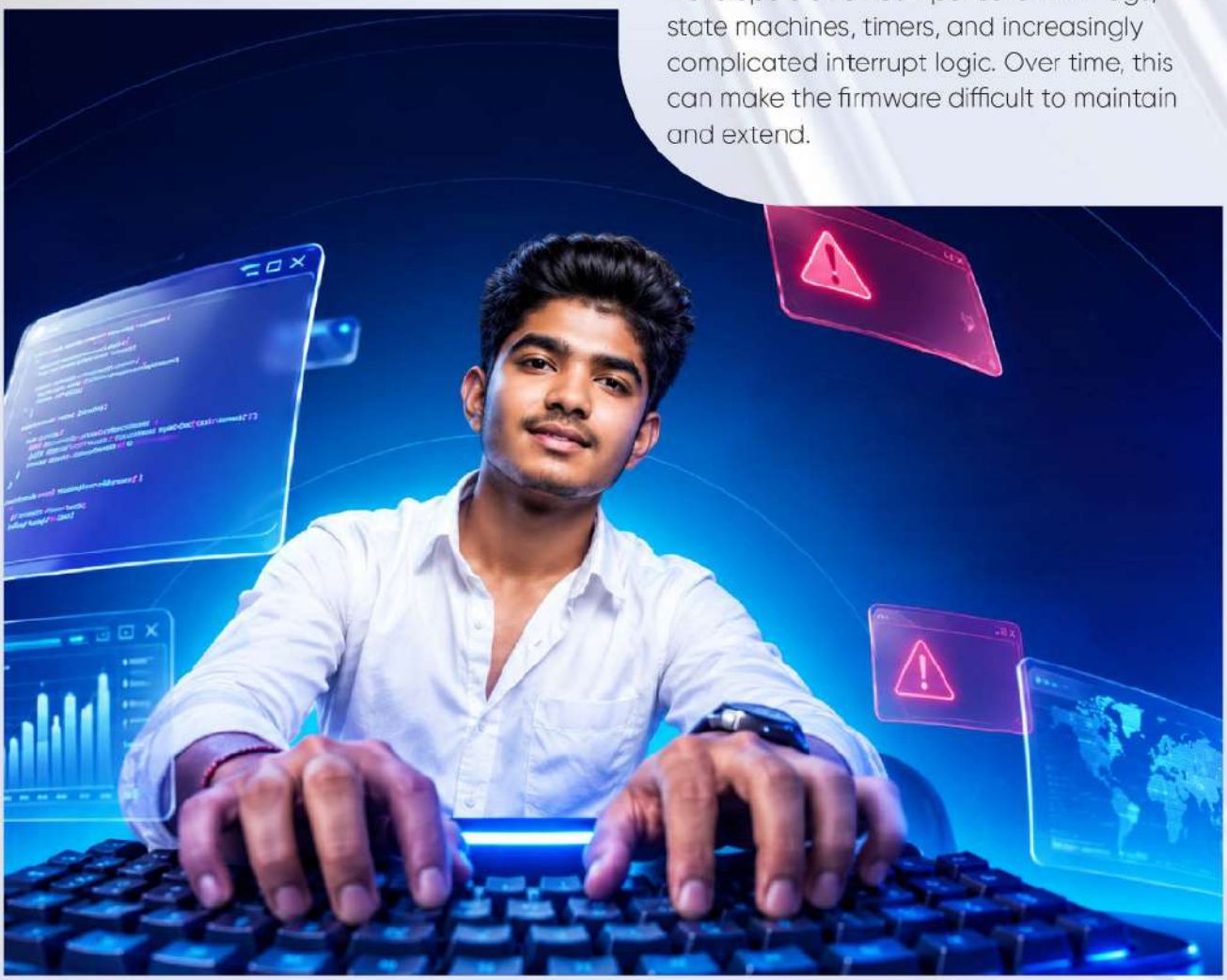
Simple debugging: Small applications are often easier to understand and troubleshoot because their execution flow is straightforward.

Power efficiency: Carefully designed firmware can spend much of its time in low-power sleep modes, making bare metal attractive for battery-operated devices.

Limitations

As applications become more complex, managing multiple activities within a single loop becomes difficult. A long-running communication routine, for example, may delay sensorprocessing or display updates.

Developers often compensate with flags, state machines, timers, and increasingly complicated interrupt logic. Over time, this can make the firmware difficult to maintain and extend.





Best suited for: Simple controllers, basic sensor interfaces, small appliances, and applications with limited concurrency and highly constrained resources.

2. Real-Time Operating Systems: Managing Multiple Tasks

A real-time operating system provides a structured way to manage multiple tasks or threads. Its scheduler determines which task should execute based on priorities and scheduling rules.

Unlike a general-purpose operating system, an RTOS is designed to support predictable timing behaviour. However, using an RTOS does not automatically guarantee that every deadline will be met. Developers must still design appropriate priorities, execution times, interrupt handling, and resource management.

RTOS platforms commonly provide tasks, queues, semaphores, mutexes, software timers, and event mechanisms. These features allow different parts of an application to communicate and coordinate safely.

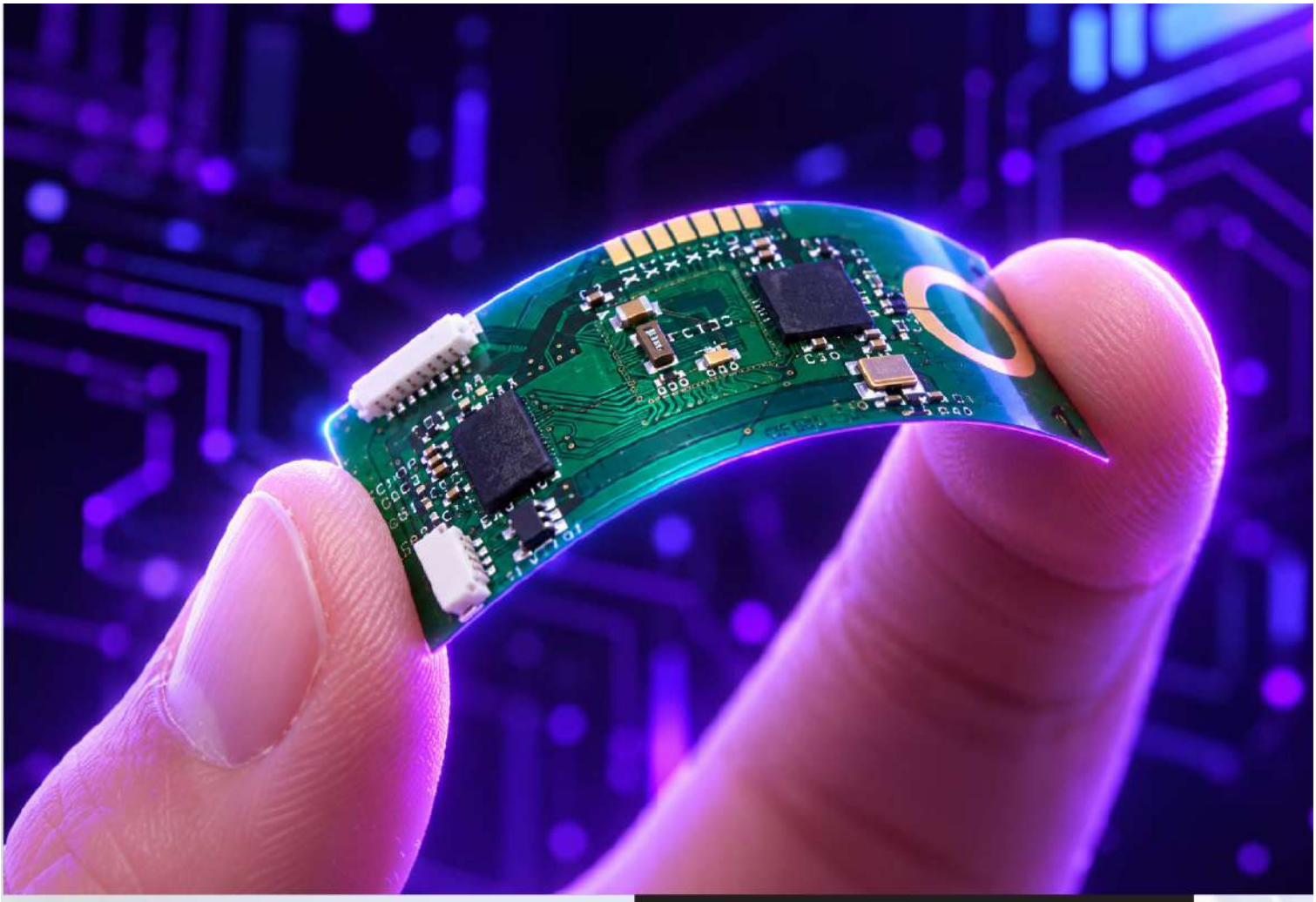
For example, an industrial monitoring device could use separate tasks for sensor acquisition, data logging, wireless communication, and display updates.

Advantages and Challenges

An RTOS improves modularity, supports concurrent activities, and makes large applications easier to organise. It can also simplify integration with networking stacks, file systems, and other middleware.

However, it introduces additional memory requirements, context-switching overhead, and greater debugging complexity. Race conditions, deadlocks, and priority inversion must be handled carefully.

Best suited for: Applications with multiple concurrent activities, communication requirements, strict timing constraints, or plans for significant future expansion.



3. FreeRTOS: Lightweight and Flexible

FreeRTOS is a widely used open-source RTOS designed for microcontrollers and resource-constrained embedded devices. Its kernel is distributed under the MIT licence, making it suitable for many commercial and educational projects.

Its core functionality includes task scheduling, queues, semaphores, mutexes, and software timers. Developers can build the application around these primitives while selecting the additional libraries and middleware their project requires.

Key Benefits

Small footprint: The kernel can be configured for systems with limited memory, although the final footprint depends on the application and enabled features.

Broad hardware support: It is available across many microcontroller architectures.

Flexible development: Developers can choose how to structure peripheral drivers, networking, and application components.

Strong learning ecosystem: Documentation, community resources, and development-board support make it accessible to beginners.

FreeRTOS is also available within Espressif's ESP-IDF framework for ESP32 development. This makes it a practical option for products that combine microcontroller control with Wi-Fi orBluetooth connectivity.

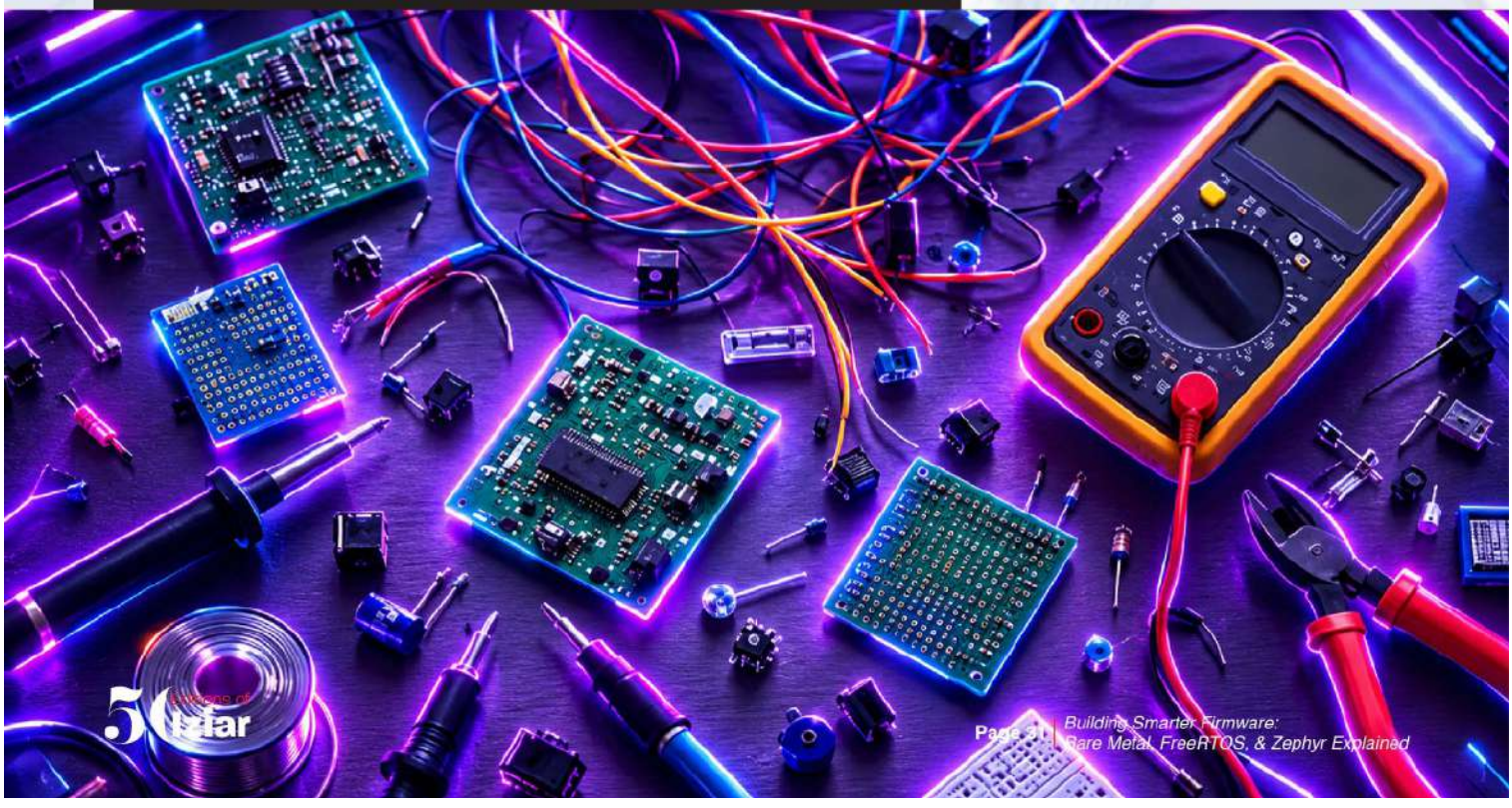
Limitations

FreeRTOS provides a lightweight kernel rather than a complete, uniform development platform. Developers may need to integrate and maintain additional components fornetworking, device configuration, security, and hardware abstraction.

Best suited for: Small to medium-sized embedded projects, ESP32 applications, STM32-based products, and teams that want RTOS functionality with considerable architectural flexibility.

4. Zephyr: **A Complete Embedded Development Platform**

Zephyr is an open-source RTOS project hosted by the Linux Foundation. Beyond task scheduling, it provides an integrated development ecosystem for building connected and portable embedded products.
Its features include hardware description through device tree, configurable software options through Kconfig, and project management using the west tool. It also provides APIs and components for areas such as networking, Bluetooth Low Energy, USB, storage, and power management.



Broad hardware support: Zephyr supports numerous development boards and microcontrollers from different vendors.

Connectivity options: Its networking capabilities make it suitable for IoT devices using technologies and protocols such as Bluetooth LE, Thread, Matter, and TCP/IP, subject to the relevant hardware and configuration.

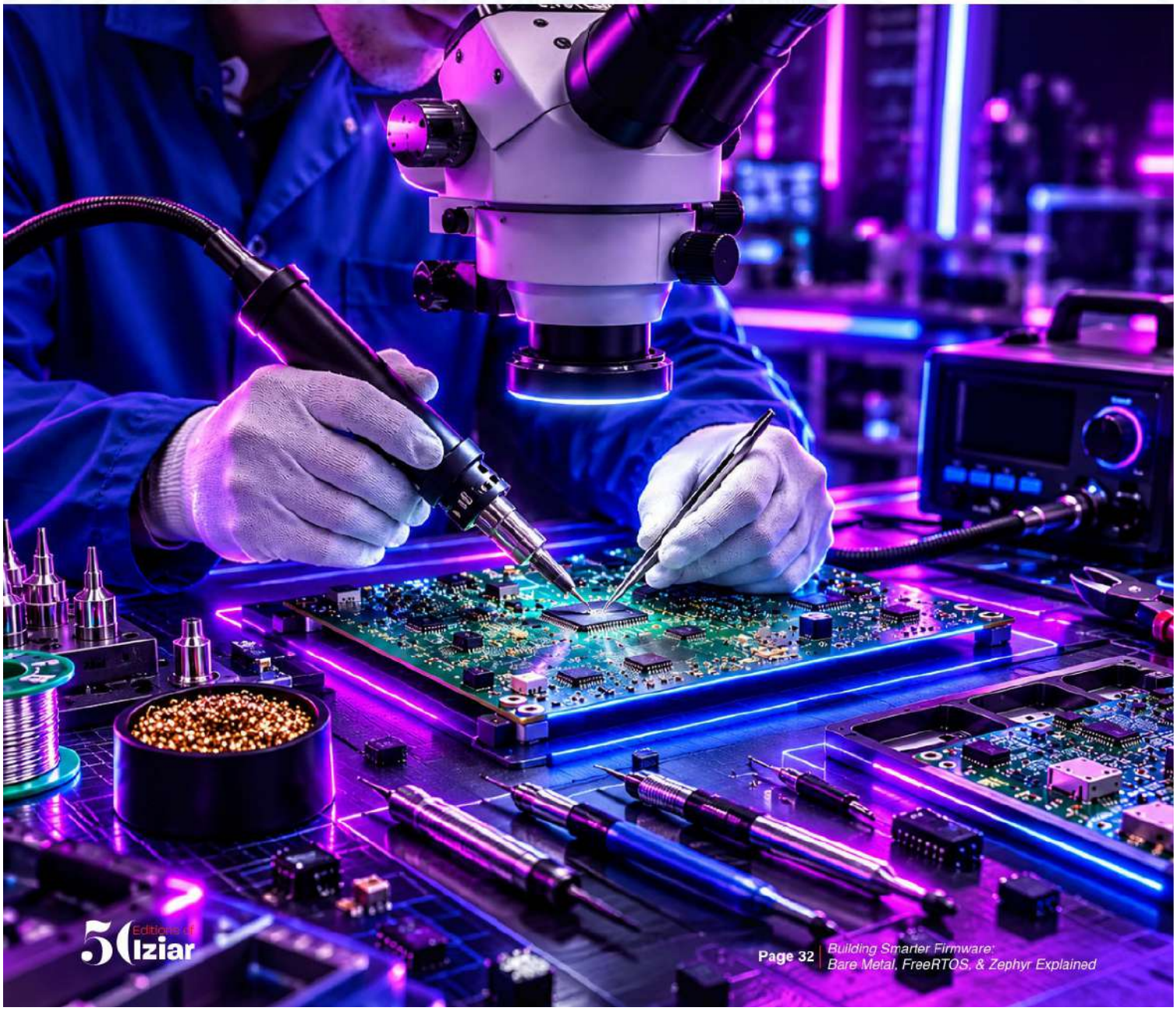
Portability: Standardised APIs can reduce the effort involved in moving applications between supported platforms.

Integrated development structure: A common configuration and build system helps teams manage increasingly complex firmware projects.

Limitations

Zephyr's extensive capabilities introduce a steeper learning curve. Developers must understand its configuration system, device tree, build process, and software architecture. Its resource requirements also vary according to the selected features and application. Although Zephyr can support constrained devices, developers must evaluate memory and performance carefully.

Best suited for: Connected IoT products, commercial devices requiring hardware portability, and applications that depend on multiple communication protocols or a structured development ecosystem.



5. Quick Comparison: Which Approach Should You Choose?

Requirement	Recommended approach
Simple device with very limited memory	Bare metal
Basic control application with few concurrent activities	Bare metal
Lightweight multitasking on an MCU	FreeRTOS
ESP32 project using Espressif"s ESP-IDF	FreeRTOS
Connected product requiring an integrated ecosystem	Zephyr
Product targeting multiple supported hardware platforms	Zephyr
Complex application with demanding timing requirements	Evaluate an RTOS and validate real-time performance

These recommendations are starting points, not strict rules. Hardware capabilities, team experience, software dependencies, security requirements, and long-term maintenance plans should also influence the decision.

6.Making the Right Engineering Decision

Before selecting an architecture, developers should answer four questions.
First, how much concurrency does the application require? If the firmware performs a few straightforward operations, bare metal may be sufficient. If several activities must progress independently, an RTOS may offer a cleaner solution.
Second, what are the resource constraints? RAM, flash, processor speed, and power consumption must be measured against the requirements of the complete application.

Third, which communication and software components are needed? Projects involving Bluetooth, networking, USB, or file systems may benefit from an RTOS platform that already provides suitable components.

Finally, how will the product evolve? Firmware intended to support new features, additional hardware, or multiple product variants benefits from a maintainable architecture.
Developers should prototype using the intended production hardware and measure execution time, memory usage, power consumption, and worst-case task response times before committing to a design.

Conclusion: Build for Today's Needs and Tomorrow's Growth

Bare-metal programming remains valuable when simplicity, low resource consumption, and
direct hardware control are the priorities. FreeRTOS provides a lightweight path to multitasking,
while Zephyr offers a more integrated platform for connected and portable embedded products.
There is no universally superior choice. The right architecture is the one that satisfies the application's timing, resource, reliability, and maintenance requirements without introducing unnecessary complexity.

A practical rule for embedded developers is to start with the simplest architecture that meets the requirements—and adopt an RTOS when concurrency, connectivity, or software complexity justifies it. Understanding the trade-offs between bare metal, FreeRTOS, and
Zephyr is an essential step towards building efficient, reliable, and scalable firmware.



IPCS® GLOBAL

www.ipcsglobal.com

BE AN IT PROFESSIONAL IN JUST 6 MONTHS!



START YOUR TECH CAREER WITH INDUSTRY-READY SKILLS.

- ***PYTHON PROGRAMMING***
- ***DATA SCIENCE***
- ***ARTIFICIAL INTELLIGENCE (AI)***
- ***DATA ANALYTICS***
- ***FULL STACK DEVELOPMENT***

Why Choose Us?

TÜV SÜD	18	100%	100%
GERMANY CERTIFICATION	YEARS OF EXCELLENCE	PRACTICAL TRAINING	PLACEMENT ASSISTANCE

JOIN THE NEXT BATCH!

Contact Us

98467 70771

Intelligent Maintenance: Fault Detection to Failure Prediction



ANJITH HARI
PROJECT ENGINEER,
IPCS GLOBAL TRIVANDRUM

Imagine a production line running smoothly when a critical motor suddenly stops. Production comes to a halt, maintenance engineers begin troubleshooting, and the factory faces unexpected downtime, repair expenses, and potential delivery delays.

In many cases, equipment provides warning signs before a failure occurs. Changes in vibration, temperature, electrical current, or operating behavior can indicate developing faults. Recognizing these changes early gives maintenance teams an opportunity to investigate problems before they lead to major breakdowns.

The Industrial Internet of Things (IIoT), combined with sensors, automation systems, and data analytics, is transforming industrial maintenance. By turning equipment data into meaningful insights, industries can improve reliability, make informed maintenance decisions, and reduce unplanned downtime.

1. Understanding the Evolution of Industrial Maintenance

Industrial maintenance has evolved from repairing failed equipment to monitoring its condition and anticipating potential problems. The main approaches include four strategies.

Reactive maintenance involves repairing equipment after a failure occurs. Although it may be suitable for low-criticality components, unexpected breakdowns in critical machinery can cause significant production losses and secondary damage.

Preventive maintenance involves servicing equipment at predetermined intervals, regardless of its actual condition. It helps reduce certain risks, but components may be replaced unnecessarily, while unexpected faults can still develop between scheduled inspections.

Condition-based maintenance relies on actual equipment measurements to determine when maintenance may be necessary. For example, a motor may be inspected when its vibration exceeds an established threshold.

Predictive maintenance uses equipment condition, historical information, operating conditions, and performance trends to estimate future deterioration or failure risk. This allows maintenance teams to plan interventions before a functional failure occurs.

Each approach has its place. The most suitable strategy depends on equipment criticality, operating conditions, maintenance costs, and the availability of reliable data.



2. How IIoT Enables Smarter Maintenance

IIoT connects industrial equipment, sensors, controllers, and software platforms to collect, transmit, and analyse operational data.
A typical system begins with sensors measuring parameters such as vibration, temperature, and electrical current. PLCs or edge gateways collect relevant signals and transfer the data to monitoring and analytics applications. Communication technologies such as OPC UA and MQTT help compatible industrial systems exchange information with monitoring platforms.
The collected data can be displayed as live readings, historical trends, and alarms. Analytics tools can then identify abnormal patterns and support maintenance decisions.
Not every application requires cloud computing or artificial intelligence. Basic condition monitoring can operate locally using controllers, alarm thresholds, and historical trends. More advanced predictive maintenance systems may use statistical analysis or machine learning to estimate failure risk.

The real value of IIoT lies not simply in collecting data, but in using it to make better engineering decisions.



3. Four Key Parameters for Monitoring Equipment Health

Vibration

Accelerometers measure vibration in motors, pumps, compressors, and other rotating machinery. Changes in vibration patterns may indicate bearing damage, shaft misalignment, mechanical imbalance, or other developing faults. Monitoring these changes helps engineers identify potential problems and plan inspections before deterioration becomes severe.

Temperature

Temperature monitoring helps identify unusual heating caused by friction, inadequate lubrication, cooling problems, or excessive loading. For example, a bearing that becomes progressively hotter under similar operating conditions may require investigation. Ambient temperature, airflow, and sensor placement must also be considered when interpreting measurements.

Electrical current

Motor current provides useful information about electrical demand and mechanical loading.
Abnormal current patterns may indicate overloading, phase imbalance, or certain electrical and process-related problems. In variable-frequency drive (VFD) applications, current readings can be analysed alongside motor speed, output frequency, and drive fault information. However, current alone cannot reliably identify every mechanical fault.



Runtime and operating cycles

Operating hours, start-stop frequency, and load history help engineers understand equipment usage. This information supports service scheduling, lubrication planning, and component replacement. For example, a pump can generate a maintenance notification after reaching a predefined number of operating hours.

Runtime-based scheduling is generally a form of preventive maintenance. When combined with actual equipment condition data, it can contribute to more advanced maintenance strategies.

4. A Practical Example: IIoT-Based Pump Monitoring

Consider a centrifugal pump driven by an induction motor in a manufacturing plant. Under reactive maintenance, the pump may continue operating until a fault causes a trip or mechanical failure. With IIoT-enabled monitoring, the system can collect bearing vibration, motor temperature, electrical current, VFD data, and operating-hour information.

Suppose the vibration level gradually increases over several days while the bearing temperature also rises under comparable operating conditions. Together, these changes provide stronger evidence of a developing problem than either measurement alone.

The monitoring system can flag the abnormal trend and notify maintenance personnel. A predictive maintenance application may compare these readings with historical data and operating conditions to estimate the likelihood of failure.

Engineers can then inspect the pump, identify the underlying cause, and schedule maintenance where necessary. Although predictions cannot guarantee that every failure will be detected, early warnings can provide valuable time to prevent avoidable downtime.



5. Condition Monitoring vs. Predictive Maintenance

Although these terms are closely related, they serve different purposes.

Condition monitoring: What is happening to the equipment right now, and how is its condition changing?

Predictive maintenance: Based on the available evidence, what is likely to happen, and what is the estimated risk or timeframe for intervention?

For example, a sensor measuring normal vibration provides condition information. A dashboard showing a steadily increasing vibration trend helps engineers understand how the equipment is changing over time. Using historical patterns and validated analytical models to estimate future failure risk takes the process towards predictive maintenance.

Simply connecting sensors to the internet or displaying live readings does not make a system predictive. Reliable predictions require good-quality historical data, an understanding of equipment failure mechanisms, suitable analytical methods, and validation against actual maintenance findings.



6. The Role of Automation Engineers

Automation engineers play an important role in connecting industrial equipment with modern maintenance applications.

PLCs collect process signals, monitor equipment status, record operating hours, and trigger alarms. SCADA and HMI systems display equipment conditions and historical trends, while VFDs provide useful information about motor current, operating frequency, and drive faults. Industrial communication technologies such as OPC UA and MQTT support the transfer of data between automation equipment and monitoring platforms. Edge devices can also process selected information locally before sending it to higher-level applications.

Successful implementation requires more than programming and communication configuration.

Engineers must consider sensor accuracy, sampling rates, data quality, network reliability, and cybersecurity. High-frequency vibration analysis, for instance, may require dedicated monitoring hardware rather than conventional PLC or SCADA measurements.

Safety is equally important. Critical machine protection, emergency stops, and safety interlocks must remain effective independently of non-critical cloud services or predictive analytics applications. IIoT should complement established protection systems, not replace them.

7. A Practical Roadmap for Implementation

Despite its benefits, predictive maintenance presents challenges, including poor data quality, legacy equipment, limited failure history, false alarms, cybersecurity risks, and implementation costs.

A structured approach can help industries adopt the technology effectively.

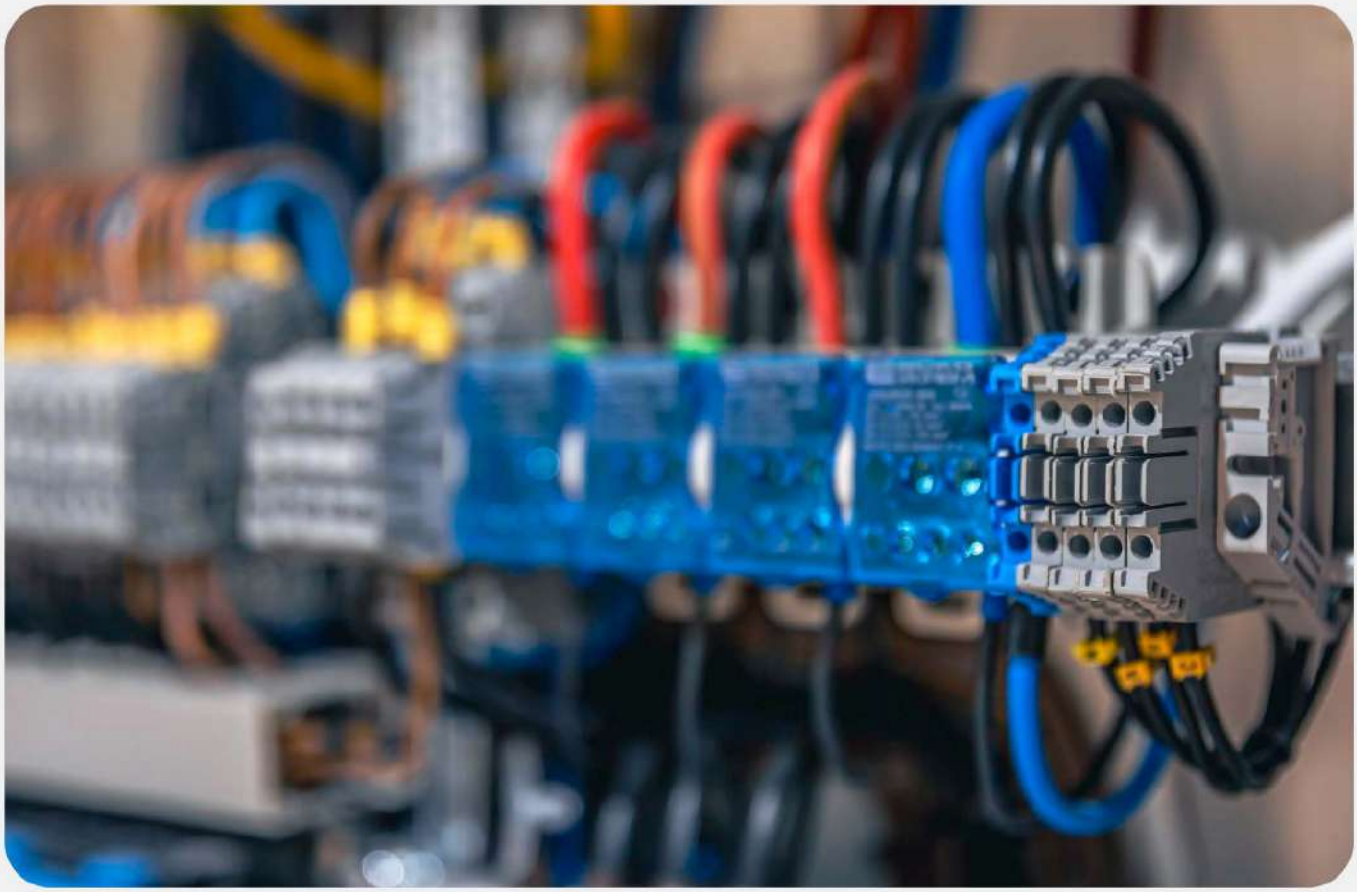
Identify critical equipment: Prioritize machinery whose failure could significantly affect production, safety, or operating costs.

Establish baseline behaviour: Record normal vibration, temperature, current, and operating conditions.

Select suitable sensors: Choose instrumentation according to equipment characteristics and anticipated failure modes.

Integrate equipment data: Use existing PLCs, VFD communication, or edge gateways wherever appropriate.

Begin with condition monitoring: Establish meaningful thresholds, historical trends, and alarm notifications.





Validate abnormal conditions: Compare monitoring results with physical inspections and confirmed maintenance findings.

Introduce predictive analytics: Develop forecasting models when sufficient reliable data is available.

Measure performance: Track unplanned downtime, maintenance costs, false alarms, and maintenance response time.

Starting with a single critical asset allows an organization to evaluate performance, identify practical challenges, and demonstrate value before expanding the system across the plant.

Conclusion: Turning Equipment Data into Action

The future of industrial maintenance is not defined by sensors or artificial intelligence alone. It depends on how effectively industries convert equipment data into useful decisions. Reactive maintenance responds to failures after they occur, preventive maintenance follows planned schedules, and condition-based maintenance uses actual equipment health to guide interventions. Predictive maintenance builds on these approaches by estimating future deterioration and failure risk.

By connecting industrial equipment with systems that collect and analyse operational information, IIoT helps maintenance teams identify abnormalities earlier, prioritize inspections, and plan interventions more effectively. For automation engineers, this shift creates opportunities to move beyond PLC programming and SCADA configuration into instrumentation integration, industrial communication, equipment diagnostics, and data analytics. Ultimately, the goal is not merely to monitor machines or predict failures. It is to understand equipment behaviour, make informed decisions, and take the right action at the right time.

Code Connect Create



ARYA SAJU
TECH LEAD,
IPCS GLOBAL KOCHI

The Future of Full Stack Development

Artificial Intelligence (AI) is transforming the technology industry. AI chatbots, intelligent assistants, recommendation systems, automated content generation, and AI-powered business applications are changing how software is developed and used. As AI tools become capable of generating code and assisting with application development, students face an important question: If AI can write code, is learning full stack development still worth it?

The answer is yes, but the role of the developer is evolving. Modern developers must do more than write code. They need to understand problems, design software systems, connect different technologies, ensure security, and build applications that deliver real value. This is where Python Full Stack Development becomes particularly relevant. By combining frontend development, backend programming, databases, APIs, and AI integration, developers can build complete applications that go beyond traditional websites.

Why Python Matters in the AI Era

Python has become an important programming language across multiple technology fields, including web development, artificial intelligence, machine learning, data science, automation, and data processing.
Its versatility creates opportunities for developers who want to combine conventional software development with AI capabilities.

Consider a student management application. A traditional version might allow students to register, log in, view courses, and submit assignments. An AI-powered version could also provide personalised learning recommendations, summarise study materials, or generate feedback on assignments.



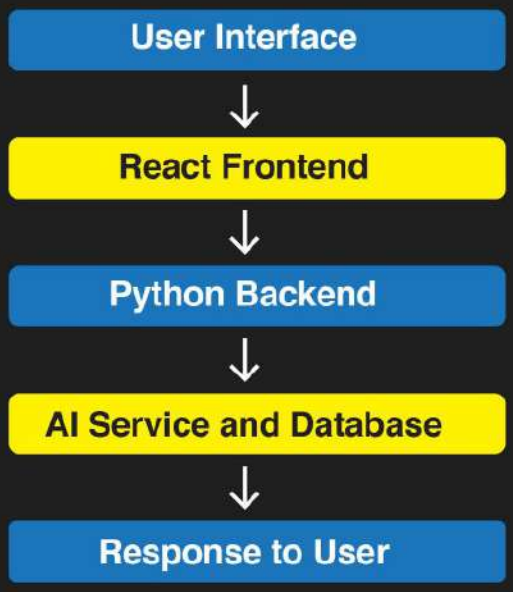
However, these additional features require more than an AI model. The application still needs a user interface, backend logic, database connectivity, authentication, and deployment.
Python helps developers build the backend and connect AI services to these essential components.

AI Models Need Complete Applications

One of the most important lessons of the AI revolution is that an AI model alone is not a complete software product.
Consider an AI-powered customer support platform. A user enters a question through a website. The frontend sends the request to a Python backend, which validates the input, communicates with an AI service, and returns the response for display.

The application may also need to authenticate users, store conversation history, manage permissions, handle errors, protect sensitive information, and monitor usage.
A typical architecture might look like this:





Each component has a specific responsibility. React can manage the interactive interface, while Python frameworks such as Django or FastAPI can handle backend operations and APIs. Databases such as MySQL or PostgreSQL store application information, and AI services provide selected intelligent capabilities.

Building a reliable application means understanding how these components work together. That is why full stack knowledge remains valuable even when AI assists with coding.

Python Full Stack and AI: A Powerful Combination

Combining full stack development with AI integration allows developers to create applications for a wide range of practical needs.

AI chat applications: Build interfaces that allow users to interact with AI models.

Intelligent learning platforms: Provide learning recommendations, study assistance, and automated feedback.

Resume and recruitment platforms: Help organise candidate information and support job matching.

Content creation tools: Develop applications that summarise, generate, or organise content.

E-commerce platforms: Integrate product recommendations and conversational shopping assistance.

Business automation systems: Connect AI services with existing applications to streamline selected workflows.

In each case, AI is only one part of the overall solution. Developers must still consider usability, performance, data management, security, and reliability.
The opportunity lies in learning to build the complete system rather than focusing on a single technology.

How the Full Stack Developer's Role Is Evolving

Traditionally, a full stack developer works across the frontend, backend, and database layers. Modern projects may also require cloud deployment, API integration, automated testing, and AI-assisted development.

A practical technology stack could include:

Frontend: HTML, CSS, JavaScript, and React.

Backend: Python with Django or FastAPI.

Database: MySQL or PostgreSQL.

Communication: REST APIs and third-party integrations.

Development tools: Git and GitHub.

Deployment: Cloud platforms and production environments.

AI integration: AI APIs, model services, and appropriate data-processing workflows.

Developers do not need to master every tool immediately. They should first understand the fundamentals and then expand their skills according to the projects they want to build.

Will AI Replace Software Developers?

AI coding tools can generate functions, explain unfamiliar code, suggest fixes, write tests, and help developers complete routine tasks more quickly.

However, building a real-world application involves decisions that go beyond code generation.

Developers must understand the problem, select an appropriate architecture, design the database, manage authentication, handle failures, protect user information, and test the application under realistic conditions.

They must also determine whether AI is genuinely useful for a particular feature. Adding an AI model without a clear purpose can increase cost and complexity without improving the user experience.





AI-generated code can also contain errors, security weaknesses, or unsuitable assumptions. Developers need enough technical knowledge to review and validate the output before using it.

The advantage belongs not simply to developers who use AI, but to those who understand software well enough to use AI effectively.

Will AI Replace Software Developers?

AI is increasingly becoming a development assistant. It can help programmers generate code, explain errors, draft documentation, create SQL queries, suggest improvements, and produce initial test cases.

These capabilities can accelerate experimentation and reduce time spent on routine activities.However, speed should not replace understanding. Developers must review generated code, run tests, check edge cases, and verify that the result meets the application's requirements.

For students, this means learning programming fundamentals remains essential. Understanding Python, object-oriented programming, databases, APIs, and application architecture makes it easier to recognise incorrect suggestions and improve AI-generated solutions.

AI should support the learning process, not become a substitute for learning.

A Practical Learning Roadmap for Students

Students aspiring to become full stack developers can follow a structured learning path.

1. Learn Python fundamentals. Understand variables, functions, data structures, object-oriented programming, and error handling.

2. Build web development skills. Learn HTML, CSS, JavaScript, and responsive design.

3. Understand backend development. Choose Django or FastAPI and learn how to create APIs and manage application logic.

4. Learn databases. Practise SQL and understand how applications store, retrieve, and update information.

5. Explore frontend frameworks. Learn React and how frontend applications communicate with backend APIs.

6. Use version control. Practise Git and GitHub to manage code and collaborate with others.

7. Learn testing and deployment. Understand debugging, automated testing, environment configuration, and cloud deployment.

8. Integrate AI capabilities. Connect an AI API to an application and learn about data privacy, response validation, usage limits, and error handling.

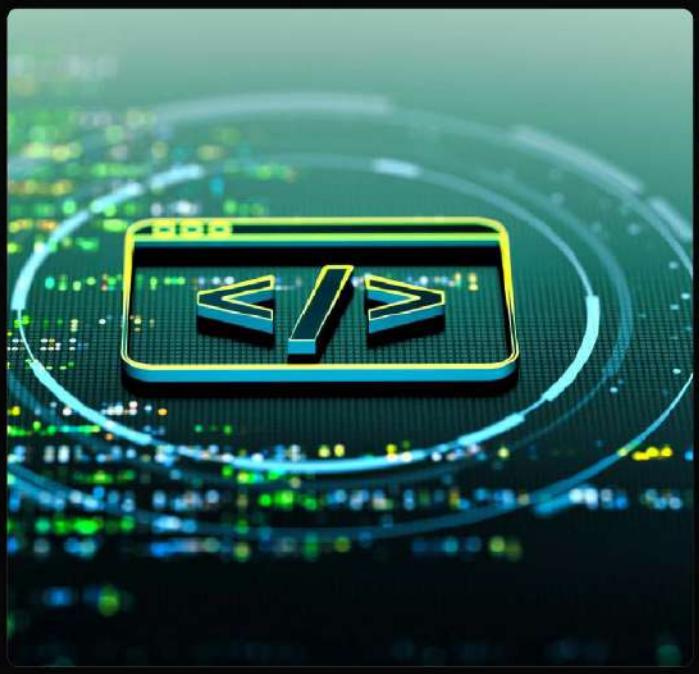
9. Build complete projects. Create practical applications, such as an AI-assisted learning portal, a customer support tool, or an intelligent inventory dashboard.

A completed project demonstrates more than familiarity with programming syntax. It shows the ability to connect technologies and solve a practical problem.



The Future of Full Stack Development

The definition of a full stack developer is expanding. Tomorrow's developers may ask not only how to build a website, but also how to create an intelligent application that solves a particular problem.Python offers a useful foundation for this direction because it supports backend development, APIs, automation, data processing, and AI-related work. Combined with frontend technologies, databases, and cloud services, it enables developers to create applications that integrate traditional software functions with intelligent features. Nevertheless, AI integration is an additional capability, not a replacement for sound engineering. Successful applications will still depend on clear requirements, thoughtful architecture, reliable code, effective testing, and responsible data handling.





Conclusion: Learn to Build with AI

The growth of artificial intelligence does not make full stack development irrelevant. Itchanges the opportunities available to developers and the skills they need to succeed. Python Full Stack Development provides a foundation for understanding how completeapplications are designed, developed, connected, and deployed. AI adds another dimension by enabling developers to introduce intelligent features and accelerate parts of thedevelopment process. For students, the best strategy is to learn the fundamentals, practise building complete applications, and gradually incorporate AI into meaningful projects. The goal should not be to compete with AI at writing code. It should be to understand technology well enough to create useful solutions with it.

Learn Python. Master the full stack. Use AI intelligently. Build solutions that solve real-world problems.

That is how developers can prepare for the next generation of software development.

ANSWERS TO ACTION
THE NEXT ERA OF AI



ADYA LEKSHMAN
IT Intern,IPCS GLOBALTRIVANDRUM

Artificial intelligence is evolving beyond answering questions and generating content. The rise of AI agents could transform how people work, make decisions, and interact with technology.

For years, artificial intelligence has helped us find information, write emails, generate images, summarise documents, and solve problems. We type a question, provide an instruction, and receive a response within seconds. Generative AI has made these capabilities accessible to millions of people, changing how we learn, communicate, and work.

However, the next stage of AI development is moving beyond generating answers. AI systems are increasingly being designed to plan tasks, use digital tools, and take action to achieve specific goals.

Imagine asking an AI assistant to organise a business trip. Instead of simply suggesting flights and hotels, the system could compare available options, check your calendar, prepare an itinerary, and organise the necessary information. With suitable integrations and permissions, it might even complete selected booking steps.

This emerging capability is known as agentic AI, and the systems designed to perform these tasks are commonly called AI agents. Together, they represent a significant shift in how humans may interact with computers



From Generating Content to Completing Tasks

The evolution of AI has progressed through several important stages. Traditional software follows predefined instructions. Machine-learning systems identify patterns and make predictions. Generative AI can produce text, images, code, and other content based on user prompts.
AI agents build on these capabilities by connecting intelligence with action.

A conventional chatbot might explain how to prepare a sales report. A generative AI system could create a report template or analyse data provided by the user. An AI agent connected to the appropriate business applications could potentially retrieve sales figures, organise the data, identify trends, generate charts, and prepare a report for review.
The difference lies in the workflow.

Traditional software follows instructions. Generative AI creates outputs. AI agents work towards objectives by planning and performing a sequence of tasks.

These categories are not entirely separate. AI agents often use generative AI models as their reasoning and language-processing components. Their distinctive feature is the ability to use tools and carry out actions rather than stopping after producing a response.

An AI agent typically combines several capabilities to complete a task.
First, it interprets the user's objective. It then divides the objective into smaller steps, determines which tools are required, and performs permitted actions. After each action, it can examine the result and decide what to do next.
For example, consider an employee who asks an AI agent to prepare a weekly sales performance report.
The agent might collect data from an authorised database, check for missing information, calculate sales totals, compare performance across periods, generate charts, and prepare a summary of important observations. The employee can then review the report before it is shared with management.







This process can reduce repetitive manual work and help employees complete tasks more efficiently.
However, an agent's effectiveness depends on the quality of its underlying AI model, the accuracy of available data, its access to the required tools, and the safeguards governing its actions. Not every agent can independently complete every stage of a complex task.

Why Are AI Agents Gaining Attention?

Modern workplaces depend on multiple digital systems, including email platforms, spreadsheets, customer relationship management software, databases, and project-management applications.
Employees often spend considerable time transferring information between these tools and completing repetitive administrative activities.
AI agents could help connect these systems and automate selected parts of business processes.

For example, a customer enquiry could trigger a workflow in which an agent retrieves the customer's previous interactions, checks relevant company policies, and prepares a suitable response for an employee to approve.
Similarly, an agent could collect information from multiple sources and prepare a summary for a project meeting.
Advances in language models, software integration, and tool use are making these possibilities
increasingly practical. Yet reliable automation still requires careful implementation, especially when tasks involve confidential information, financial decisions, or critical business operations.
The opportunity is not simply to make computers faster. It is to reduce the number of manual steps required to accomplish a task.

AI Agents Transforming the Workplace

AI agents could influence several professional fields.

Customer service: Agents can help retrieve customer information, classify enquiries, suggest solutions, and prepare responses. Complex complaints and sensitive cases may still require human intervention.

Finance and accounting: Agents could assist with organising financial records, preparing summaries, identifying unusual transactions, and highlighting discrepancies for further investigation.

Human resources: Interview scheduling, candidate documentation, onboarding support, and routine employee enquiries are examples of activities that could benefit from agent-based automation.

Digital marketing: Agents could help research audiences, analyse campaign performance, organise content calendars, and prepare draft marketing materials. Human creativity and brand judgement remain important.

Software development: AI agents can assist with code analysis, bug identification, testing, documentation, and selected development tasks. Their output must be reviewed, particularly when software security and reliability are involved.

Industrial automation may also benefit from agentic AI. In manufacturing environments, AI agents could potentially assist with analysing production data, preparing maintenance reports, identifying unusual operating patterns, and supporting troubleshooting workflows. However, direct control of machinery or safety-critical equipment requires specialised engineering safeguards and must not be treated like an ordinary office automation task.



The Rise of the Digital Workforce

One emerging concept is the digital worker: software designed to perform a defined set of computer-based activities. An organisation might deploy one agent to organise customer requests, another to prepare daily reports, and another to check documents for errors. Specialised agents could also collaborate on larger workflows, with each handling a particular responsibility. This approach could create a new kind of digital team in which employees work alongside AI systems.

Humans would establish objectives, provide context, review important results, and make consequential decisions. AI agents would handle suitable repetitive tasks and support information processing. The goal should not be to automate every activity. Instead, organisations need to identify where AI can create measurable value without compromising accuracy, security, or service quality.

Can AI Agents Be Trusted?

The ability to take action introduces risks that go beyond generating incorrect information.

A chatbot might provide an inaccurate answer, but an AI agent with access to business applications could potentially send an incorrect email, modify a database, expose confidential information, or make an unauthorised purchase. Agents may misunderstand instructions, produce unreliable results, or respond unexpectedly when circumstances change. They can also be vulnerable to malicious instructions embedded in external content if their systems are not designed to resist such attacks. Responsible implementation therefore requires strong controls.



Organisations should provide agents with only the permissions necessary for their assigned tasks. High-impact actions should require human approval where appropriate. Important activities should be recorded and monitored, and systems should be tested before being introduced into critical workflows.

Trust should be built through demonstrated reliability, not assumed simply because a system uses advanced AI.

Will AI Agents Replace Human Jobs?

The growth of agentic AI raises concerns about employment. Some repetitive and predictable digital tasks may become automated, changing the responsibilities associated with many jobs.

However, automating individual tasks does not necessarily mean eliminating entire professions.

Many roles involve communication, problem-solving, leadership, ethical judgement, and decisions that require an understanding of human circumstances.

As AI capabilities expand, professionals may need to develop new skills. These include writing clear instructions, verifying AI-generated information, evaluating results, protecting sensitive data, and supervising automated workflows.

There may also be growing demand for people who can integrate AI tools into existing business processes, assess their performance, and manage the risks associated with their use.

The important question is not only whether AI will replace certain tasks, but also how people can adapt their skills to work effectively with these systems.

The Human Advantage in an AI-Driven World

Despite rapid technological progress, human judgement remains essential.

Empathy helps us understand other people. Creativity allows us to approach unfamiliar problems in new ways. Ethical reasoning helps us evaluate competing priorities, while leadership and accountability guide decisions that affect individuals and organisations.

AI agents can provide information, recommendations, and operational support, but their outputs still need to be evaluated in context.

The most effective future may involve collaboration rather than competition: machines handling appropriate tasks while people provide direction, assess outcomes, and remain accountable for important decisions.



Conclusion: A New Relationship with Technology

Artificial intelligence has already changed how we access information and create digital content.

AI agents could take this transformation further by changing how work gets done.

Instead of manually managing every step of a process, users may increasingly define an objective and delegate selected activities to AI systems. This could reduce repetitive work, connect digital applications, and give professionals more time to focus on complex and meaningful responsibilities.

However, the future of AI agents will depend on more than technological capability. Reliability, privacy, security, accountability, and human oversight will determine whether these systems become genuinely useful partners.

For students, professionals, and organisations, the next step is to understand both the opportunities and the limitations of agentic AI

We are moving towards a future where interacting with AI may mean more than asking a question and receiving an answer. It may mean defining a goal, delegating the work, and reviewing the result.

The next era of AI will not be measured only by how intelligently machines respond, but by how responsibly and effectively they help us turn intentions into action.



1MILLION+

GLOBAL PLACEMENTS

AND STILL COUNTING!



IFCS® GLOBAL

JOIN NOW

EMI OPTION AVAILABLE

+91 9846 770 771



When Quantum Computing Challenges Cybersecurity



NANDHAKUMAR
TECH LEAD,
IPCS GLOBAL COIMBATORE

The next generation of computing could transform science and technology—but it may also force the world to rethink how digital information is protected.

Every time we make an online payment, send a private message, access a cloud platform, or log in to a secure website, we rely on encryption to keep our information safe. Much of this protection depends on mathematical problems that are extremely difficult for today's computers to solve. For decades, this has been the foundation of digital security.

But what happens when a new kind of computer can solve some of these problems far more efficiently?

That is the question emerging around quantum computing. Although the technology is still developing, its potential impact on cybersecurity is already attracting the attention of governments, technology companies, researchers, and security professionals worldwide. A sufficiently powerful quantum computer could eventually undermine some of the encryption methods that protect sensitive information across the internet.

The challenge is not simply about building faster computers. It is about preparing for a future in which the rules of digital security may need to change.



A Different Way of Computing

Traditional computers, from smartphones to supercomputers, process information using bits. Each bit represents either a 0 or a 1. By combining these binary values, computers perform everything from basic arithmetic to complex scientific simulations.

Quantum computers operate according to the principles of quantum mechanics, using units of information called qubits.

Two important quantum properties help explain how they work: superposition and entanglement. Superposition allows a qubit to exist in a quantum state that combines the possibilities of 0 and 1.

For everyday activities such as browsing websites, editing documents, or streaming videos, classical computers remain the practical choice. Quantum computers are being developed for specialised problems where their unique capabilities may offer a significant advantage.

One area of particular concern is cryptography. Some of the mathematical problems that underpin today's digital security could become much easier to solve with a sufficiently advanced quantum computer.

Entanglement creates correlations between quantum systems that cannot be described in the same way as ordinary classical systems. Together with carefully designed quantum operations, these properties enable quantum computers to solve certain problems in fundamentally different ways from conventional machines.

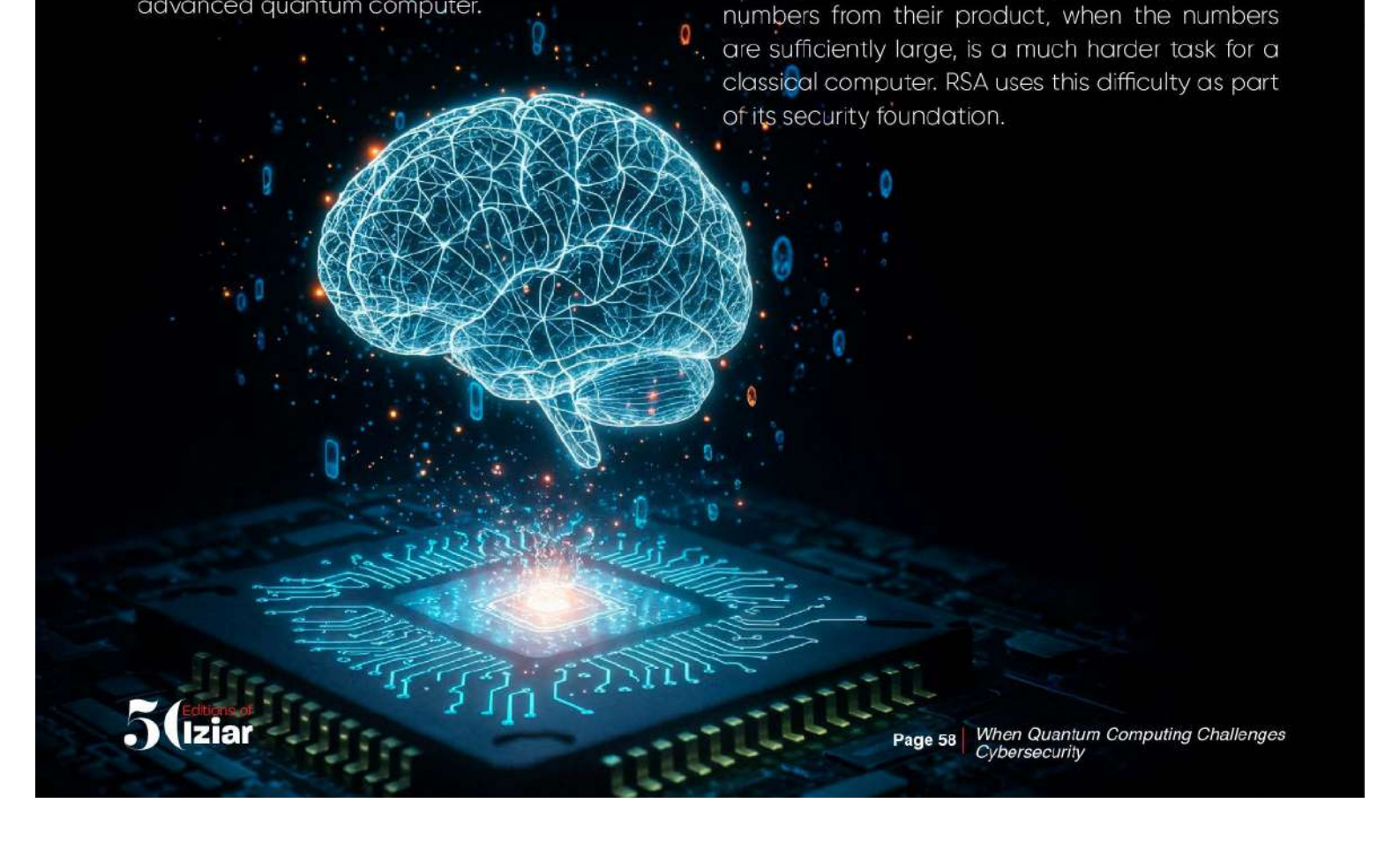
However, quantum computing does not mean that every possible answer can simply be calculated and read at once. Quantum algorithms must be designed to make useful answers more likely when a measurement is performed.

Why Today's Encryption Could Be at Risk

Much of the internet's security relies on public-key cryptography. Technologies such as RSA and elliptic-curve cryptography (ECC) help establish secure connections, exchange encryption keys, and verify digital identities.

These systems rely on mathematical problems that are easy to perform in one direction but extremely difficult to reverse using conventional computers.

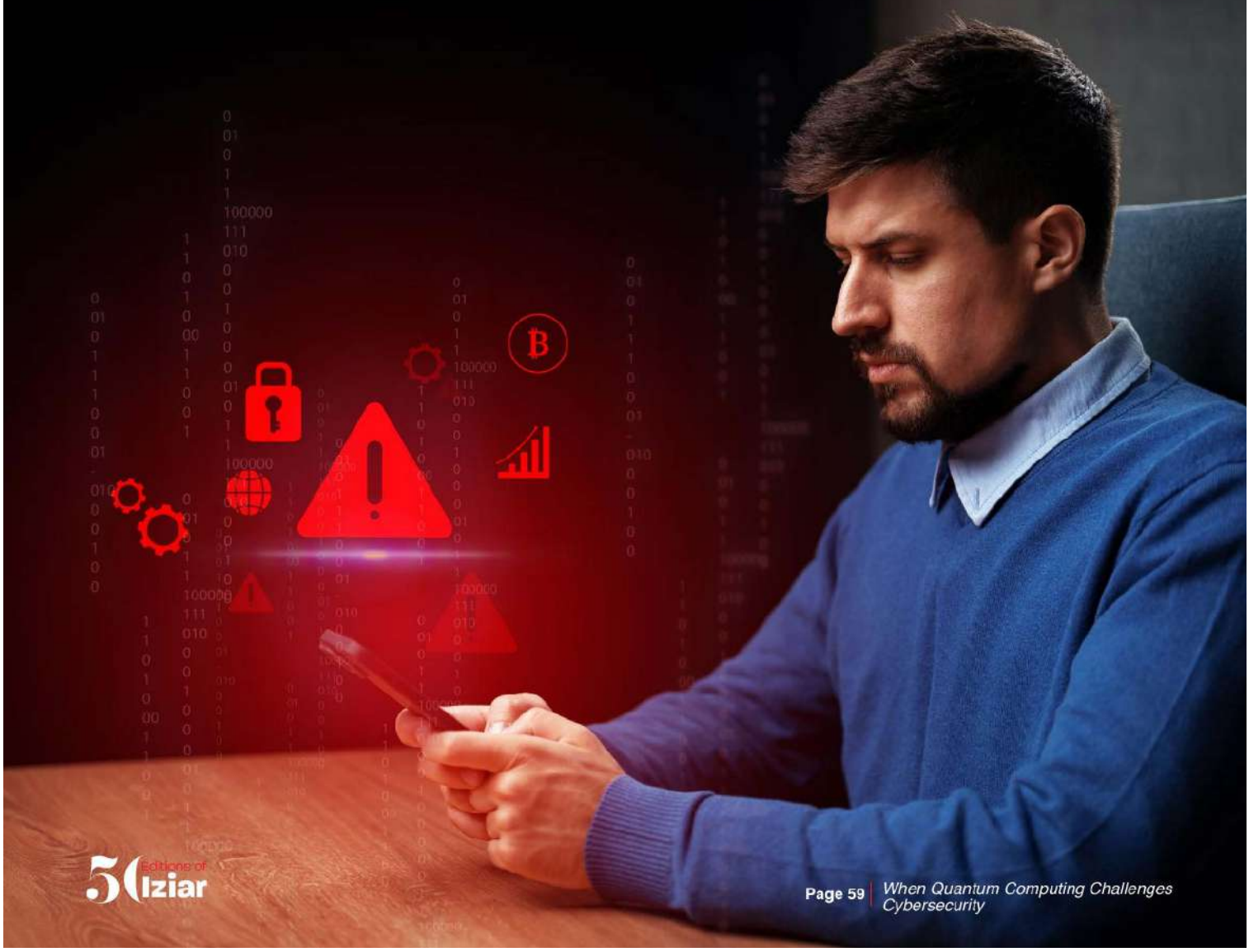
For example, multiplying two large prime numbers is straightforward. Recovering those original prime numbers from their product, when the numbers are sufficiently large, is a much harder task for a classical computer. RSA uses this difficulty as part of its security foundation.



Quantum computing introduces a potential weakness in this arrangement. In 1994, mathematician Peter Shor developed an algorithm that demonstrated how a sufficiently powerful quantum computer could factor large integers and solve certain discrete logarithm problems much more efficiently than the best known classical approaches.

If a large, fault-tolerant quantum computer becomes capable of running this algorithm against real-world cryptographic keys, widely used systems such as RSA and ECC could become vulnerable. The consequences would extend beyond individual accounts to secure communications, financial infrastructure, digital identity systems, and government networks. The term Q-Day is often used to describe the point at which quantum computers become practically capable of breaking cryptographic systems that are widely used today.

That milestone has not yet been reached. Today's quantum processors face major challenges involving noise, errors, and the difficulty of maintaining reliable quantum operations at scale. The number of physical qubits alone does not determine whether a machine can break modern encryption; the quality of those qubits, error correction, and the resources required by a particular algorithm are also critical. When Q-Day might arrive remains uncertain. Nevertheless, security planning cannot depend entirely on waiting until the technology is ready. The time required to upgrade complex digital systems makes early preparation essential.



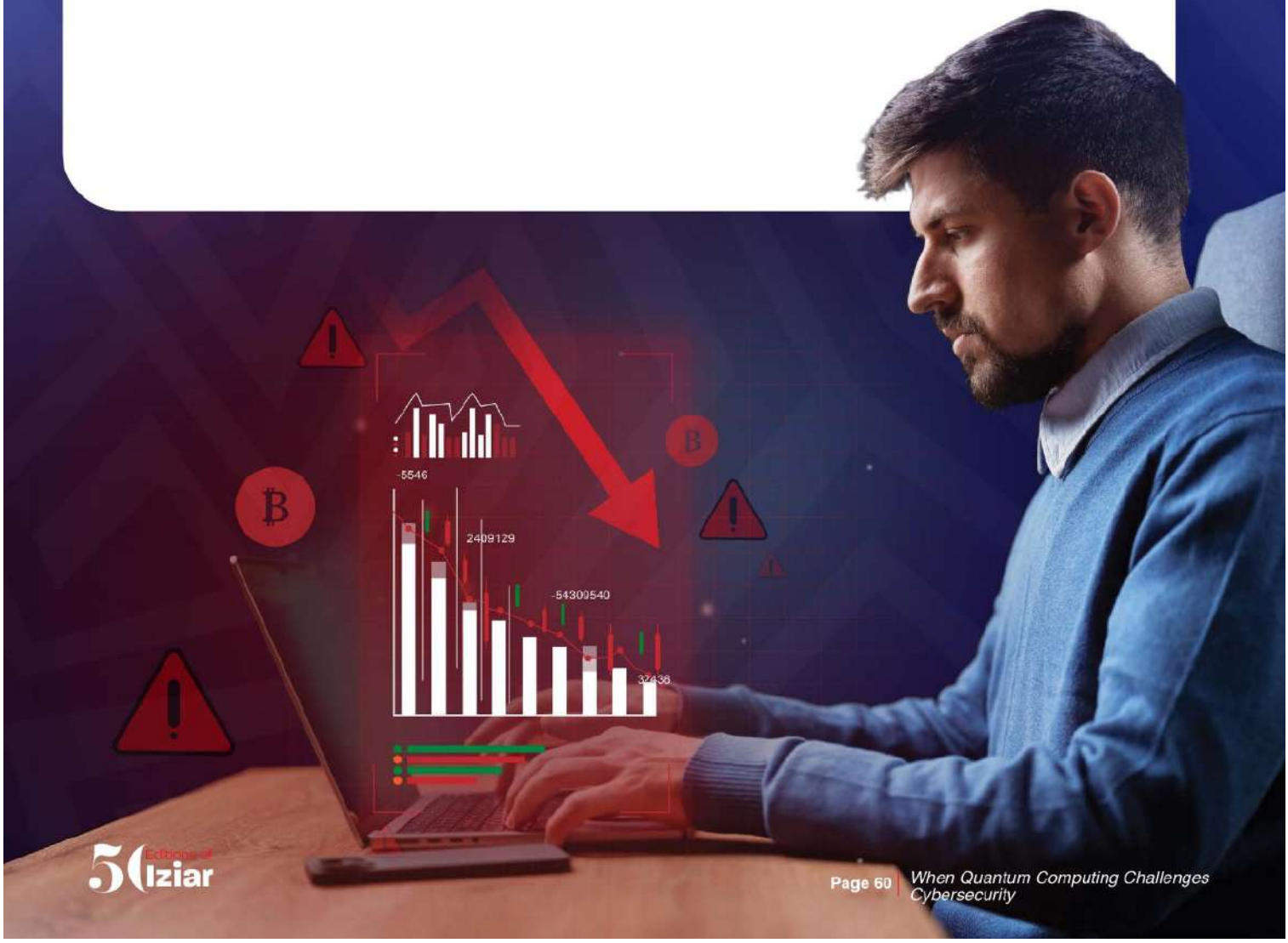
The Hidden Risk: Harvest Now, Decrypt Later

One of the most important cybersecurity concerns associated with quantum computing is known as "harvest now, decrypt later." The idea is simple: an attacker collects encrypted information today and stores it, hoping to decrypt it in the future when more powerful quantum computers become available. Consider a confidential government communication or a medical record transmitted in 2026.

Even if the information cannot be decrypted today, an attacker could retain a copy. If the encryption method becomes vulnerable in the future, that previously captured information could potentially be exposed.

This makes the threat particularly serious for information that must remain confidential for many years. Examples include:

- Medical records and sensitive personal information.
- Government communications and national security documents.
- Intellectual property, research data, and trade secrets.
- Financial records and confidential business agreements.
- Long-term strategic plans and legal documents.



Post-Quantum Cryptography: Preparing for a New Era

Researchers are already working on ways to defend digital systems against future quantum attacks. One of the most important developments is post-quantum cryptography (PQC).

Unlike conventional quantum computing, PQC does not require a quantum computer. These cryptographic methods are designed to run on ordinary computers while resisting attacks from both classical and known quantum algorithms.

Instead of relying on mathematical problems that Shor's algorithm can solve efficiently, post-quantum algorithms use other mathematical structures believed to remain difficult for quantum computers to attack. These include lattice-based problems and approaches involving hash functions.

The US National Institute of Standards and Technology (NIST) has led a major international effort to evaluate and standardise post-quantum cryptographic algorithms. Its standards provide organisations with a practical foundation for beginning the transition to quantum-resistant security.

However, adopting these methods is not as simple as installing a software update. Large organisations often depend on hundreds of applications, network devices, cloud services, databases, and third-party platforms. Cryptography may be embedded in systems that are difficult to identify or update. New algorithms must also be tested for compatibility, performance, and operational reliability.

During the transition, some systems may use hybrid approaches that combine established cryptographic methods with post-quantum alternatives. This can provide a practical migration path, although the security of the overall design depends on how the combination is implemented.

The transition will require coordination across the technology industry, financial institutions, governments, and software developers. Starting early gives organisations more time to identify weaknesses, test solutions, and address compatibility problems before quantum threats become more immediate.



Quantum Key Distribution:
Using Physics for Protection

Post-quantum cryptography changes the mathematical foundations of security. Quantum key distribution (QKD) takes a different approach by using the physical properties of quantum systems to help two parties establish a shared secret key.

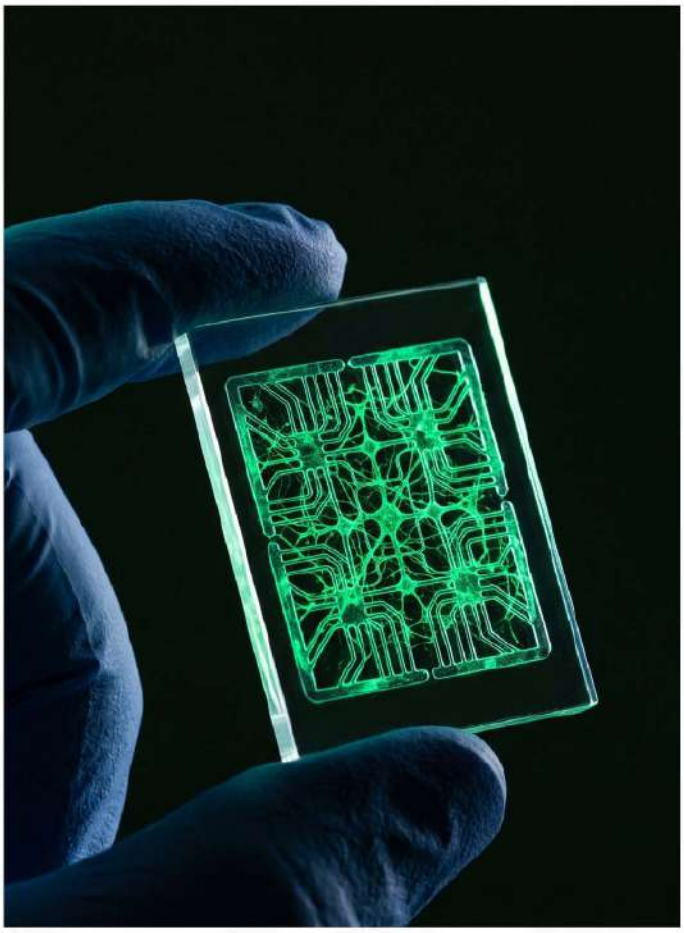
QKD commonly uses photons, or particles of light, to transmit quantum information. Measuring a quantum state can disturb it, allowing certain interception attempts to be detected under the protocol's assumptions and when the equipment operates correctly.
This offers an interesting alternative to security methods based entirely on mathematical difficulty. Instead, QKD uses principles of quantum physics to help detect eavesdropping during key distribution.

However, the technology has practical limitations.

QKD requires specialised equipment and suitable communication links, such as dedicated optical fibre or satellite-based systems. Distance, infrastructure costs, and hardware requirements can make deployment challenging. In addition, real-world security depends on implementation, device quality, and protection against attacks that exploit weaknesses outside the ideal theoretical model.

For these reasons, QKD is not expected to replace ordinary internet encryption across the board. It may be useful in specialised, high-security applications, such as selected government communications or links between important data centres.

For many organisations, post-quantum cryptography offers a more practical route because it can be incorporated into existing computing infrastructure without requiring quantum communication hardware. The two approaches address related challenges, but they serve different purposes and may complement one another.





How Organisations Can Prepare

Preparing for quantum-related cybersecurity risks requires more than purchasing new technology. It calls for a planned transition that begins with understanding how an organisation currently protects its information.

1. Identify where cryptography is used

Organisations should create an inventory of encryption methods, digital certificates, authentication systems, applications, network devices, and third-party services. Without this overview, critical dependencies may remain hidden.

2. Prioritise sensitive information

Systems protecting data that must remain confidential for many years deserve particular attention. Organisations should assess the potential consequences of future decryption, the value of the information, and the length of time it needs protection.

3. Plan the transition to post-quantum standards

Security teams should follow recognised standards and guidance, test suitable post-quantum algorithms, and develop a realistic migration plan. High-risk systems may need attention before less critical applications.

4. Build crypto-agility into systems

Crypto-agility is the ability to replace or update cryptographic algorithms without redesigning an entire system. This flexibility can help organisations respond not only to quantum computing but also to newly discovered weaknesses in existing cryptographic methods.

5. Test compatibility and performance

New cryptographic methods can affect processing requirements, network traffic, storage, and system compatibility. Pilot projects and controlled testing can help identify issues before large- scale deployment.

6. Work with technology providers

Organisations depend on software vendors, cloud providers, hardware manufacturers, and communication platforms. Coordinating with these providers helps ensure that upgrades are supported throughout the technology supply chain. The objective is not to predict the exact date of Q-Day. It is to reduce dependence on vulnerable systems and make the transition manageable before urgent changes become unavoidable.

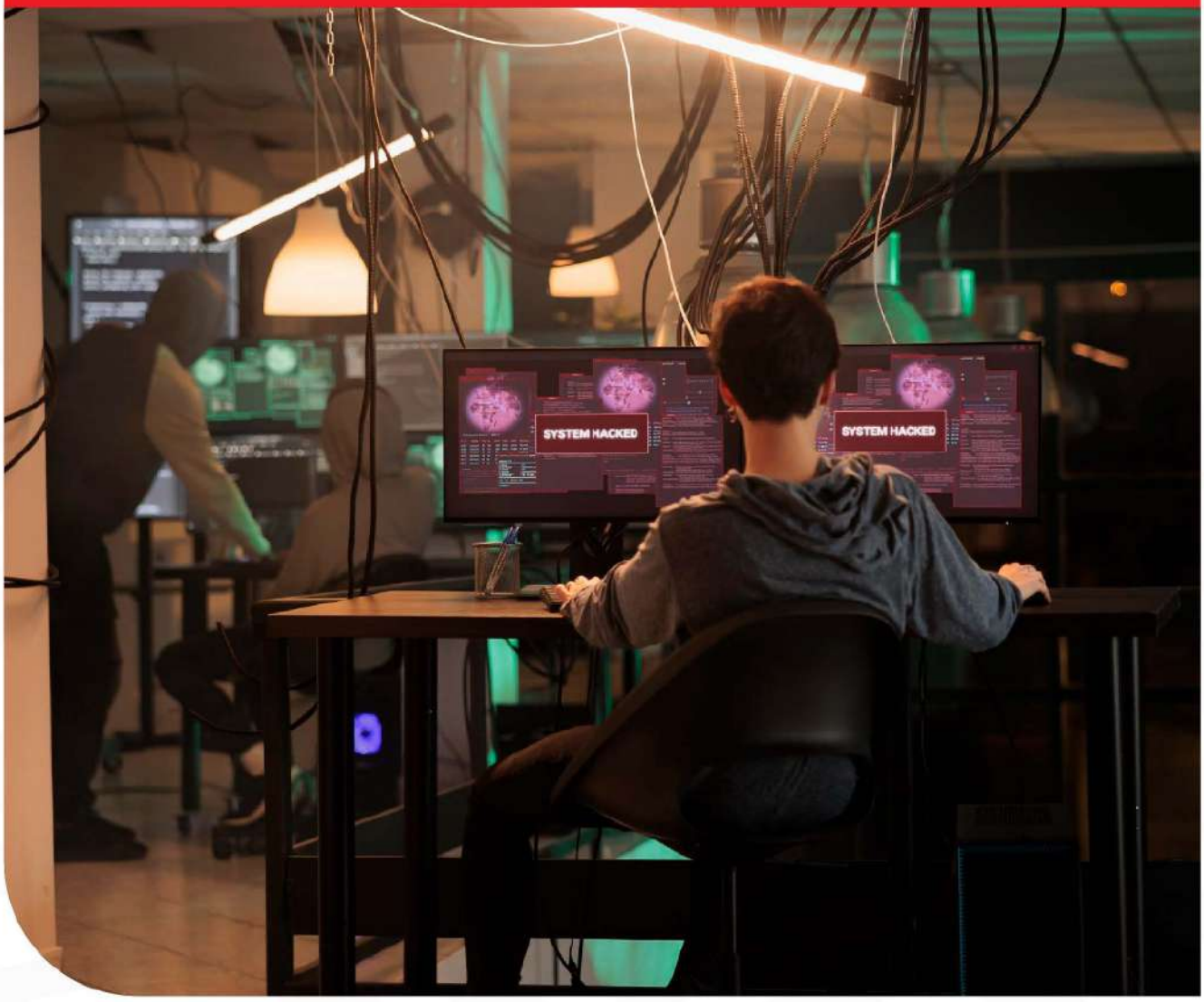
The Road Ahead

Quantum computing presents cybersecurity with a difficult challenge, but it also offers an opportunity to strengthen the way digital systems are designed and protected. The technology could eventually undermine important cryptographic methods used across the internet. At the same time, research into post-quantum cryptography and quantum-based security techniques is creating new ways to defend sensitive information.

The immediate priority is to recognise that cybersecurity must look beyond today's threats. Information captured now may remain valuable in the future, and replacing cryptographic systems across a large organisation can take considerable time.

For businesses, governments, technology professionals, and students entering the cybersecurity field, understanding quantum computing is becoming increasingly relevant. The future will require people who can evaluate emerging risks, implement new standards, and design systems that remain secure as technology evolves.

Quantum computing may change the way the world approaches digital trust. Whether that change becomes a major security crisis or a catalyst for stronger protection will depend, in large part, on the preparations made today.



From Hijacking to Account Takeover: Defending the Digital Identity



ANJALI A
IT ENGINEER,
IPCS GLOBAL TRIVANDRUM

Attackers no longer need to break down the front door. Sometimes, they simply wait for someone to open it and follow them inside. In today's digital world, stealing a password is only one way to gain access. Criminals can also hijack active sessions, exploit weak account recovery processes, or misuse trusted applications to take control of digital identities. This threat is known as account takeover (ATO). Preventing it requires organisations to look beyond the login page and secure the entire authentication journey, from account creation to sign-in, session management, recovery, and incident response.

Why Login Security Is No Longer Enough

Traditionally, authentication relied on usernames, passwords, and sometimes a one-time verification code. Once a user successfully signed in, systems generally trusted the resulting session. Attackers have learned to exploit this trust. They may obtain credentials from data breaches, steal passwords through phishing, or use malware to collect browser cookies and authentication tokens. These tokens can allow them to access an account without repeating the original login process.



A compromised session becomes particularly dangerous when attackers use it to establish long term access. They may register their own multi-factor authentication (MFA) device, create email-forwarding rules, approve malicious applications, or generate persistent access tokens. The lesson is simple: successful authentication does not guarantee that the person using the account is still its legitimate owner.

How an Account Takeover Happens

Although techniques vary, many account takeover attacks follow a similar sequence.

1. Reconnaissance: Attackers identify potential victims and discover which services or identity providers they use.
2. Credential theft: Passwords are obtained through phishing, malware, password reuse, or previously leaked databases.
3. Authentication bypass: Criminals exploit weaknesses in MFA, manipulate users into approving requests, or intercept verification codes.
4. Session hijacking: Stolen cookies or tokens are used to access an already authenticated account.
5. Persistence: Attackers add authentication methods, create malicious application permissions, or establish other ways to regain access.
6. Exploitation: The compromised account is used for financial fraud, data theft, further intrusion, or resale to other criminals.

Each stage offers an opportunity for detection and prevention. Organisations become vulnerable when they protect the initial login but overlook what happens afterwards.



Common Techniques Behind Modern Account Takeover

Credential stuffing and password spraying exploit weak password practices. Credential stuffing uses stolen username-password combinations against other services, while password spraying tests a small number of common passwords across many accounts.

Adversary-in-the-middle phishing takes traditional phishing a step further. A fraudulent website relays information between the victim and the genuine login service, potentially capturing the session cookie after the victim completes MFA. The attacker may then reuse the stolen session.

MFA fatigue involves repeatedly sending approval requests until a user accepts one, sometimes after receiving a convincing call from someone pretending to be technical support. Number matching and phishing-resistant authentication can reduce these risks.

Infostealer malware collects sensitive information from infected devices, including saved passwords and browser session cookies. Unmanaged personal devices can increase organisational exposure when they are permitted to access business applications.

OAuth consent phishing targets application permissions rather than passwords. A user may unknowingly authorise a malicious application to access email, documents, or contacts. Depending on the permissions and token configuration, this access may continue even after a password change.





Finally, **weak account recovery** can undermine otherwise strong security. If a help desk resets MFA after a brief phone conversation or an account can be recovered using easily discovered personal information, attackers may bypass the strongest login controls.

Why Multi-Factor Authentication Needs an Upgrade

MFA remains essential, but not all authentication methods provide the same level of protection. SMS codes, voice calls, and conventional authenticator codes can sometimes be intercepted or entered into convincing fake websites.

Passkeys and hardware security keys using FIDO2 and WebAuthn provide stronger protection against phishing. They use cryptographic credentials associated with the legitimate website or application. A fake domain cannot simply collect a passkey response and replay it against the genuine service.

Organisations should prioritise phishing-resistant MFA for administrators, finance teams, and other high-risk users, while gradually expanding adoption across the workforce.

Securing Authentication from Start to Finish

Protecting digital identities requires a layered approach.

1. Account enrolment: Verify identity according to the account's risk level, reject known compromised passwords, and encourage phishing-resistant authenticators. Provide secure backup authentication options without creating weak recovery shortcuts.

2. Sign-in: Apply rate limits to prevent automated password attacks. Use passkeys or security keys wherever possible, and evaluate contextual signals such as device health, unusual locations, and suspicious login behaviour.

3. Session management: Treat session cookies and tokens as credentials. Use secure cookie settings, limit session lifetimes according to risk, rotate session identifiers when privileges change, and invalidate active sessions on sign-out or suspected compromise. Require fresh authentication before sensitive actions such as changing recovery details or registering a new MFA device.

4. Application and token security: Apply secure OAuth and OpenID Connect practices, including authorisation code flow with PKCE where appropriate, strict redirect URI validation, and proper state and nonce checks. Restrict application permissions, rotate refresh tokens, and monitor for suspicious token reuse.

5. Account recovery: Require strong identity verification before resetting credentials or MFA. Remove security questions where possible, use a separately registered verification channel, and require additional approval for privileged accounts. Notify users whenever recovery details or authenticators change.

6. Detection and response: Monitor for suspicious activity, including unfamiliar devices, unexpected MFA registrations, new mailbox-forwarding rules, unusual application permissions, and large data downloads. When a takeover is suspected, revoke sessions and tokens, reset credentials, remove attacker-controlled authentication methods, and investigate possible lateral movement.



Authentication security is moving towards passwordless sign-in, stronger session protection, and continuous risk assessment. Device-bound session technologies can make stolen cookies harder to reuse on another machine, while better token controls can reduce the value of leaked credentials.

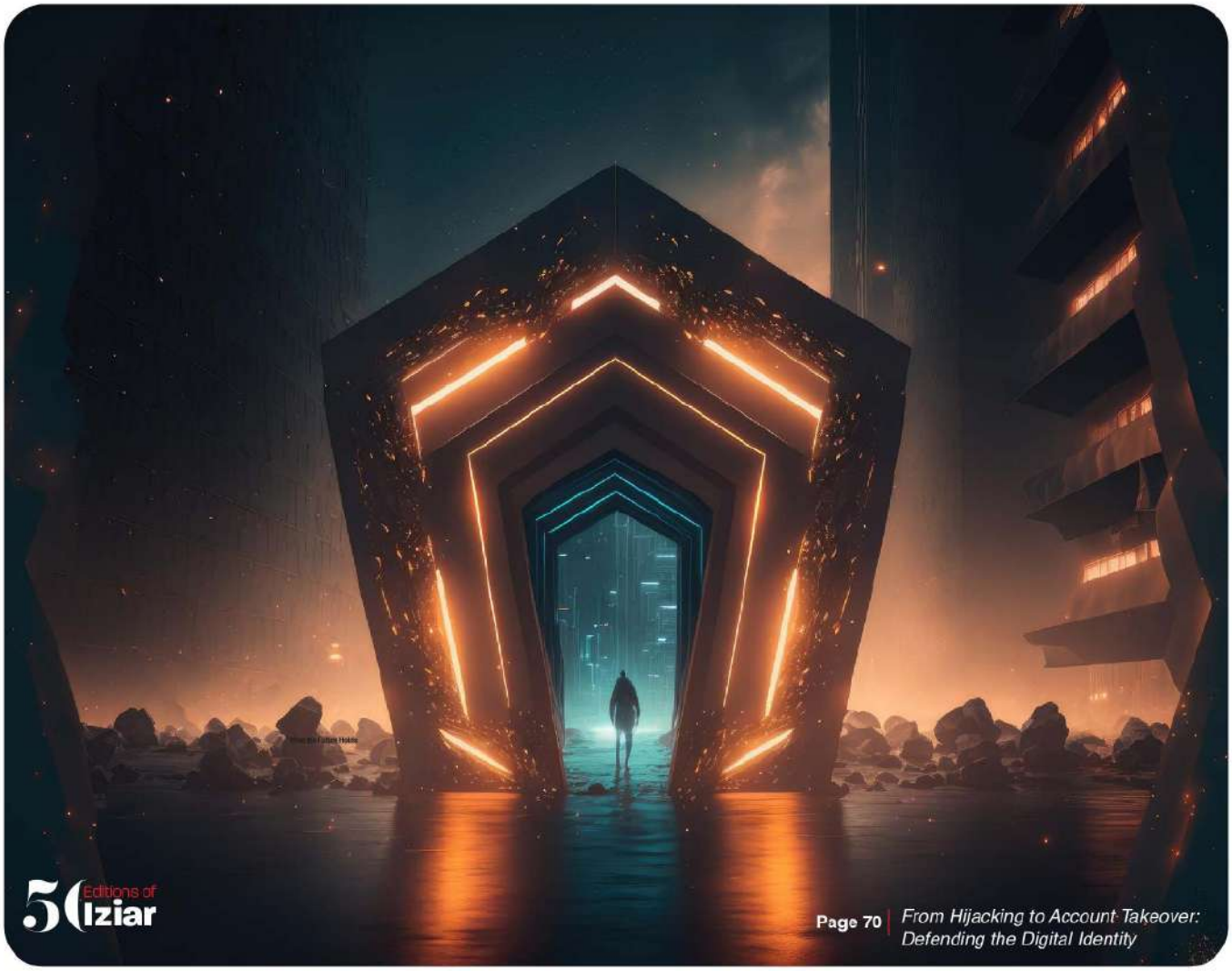
The growing use of AI agents and automated services introduces another challenge: machine identities also need secure credentials, restricted permissions, and continuous monitoring.

Organisations must ensure that both human and machine accounts receive only the access they need.

Conclusion: Protect the Journey, Not Just the Gate

Account takeover succeeds when attackers exploit gaps between security controls. A strong password cannot prevent every phishing attack, MFA cannot protect every stolen session, and a secure login cannot compensate for weak recovery procedures.

The solution is to protect the complete authentication lifecycle. By combining phishing-resistant MFA, secure session and token management, strong recovery processes, and continuous monitoring, organisations can make account takeovers harder to execute and easier to detect.



IFCS GLOBAL

www.ipcsglobal.com

Want an International Career?



Get Industry-Ready Skills in Industrial Automation with a **Global Certification!**

• PLC • SCADA • VFD • HMI

- TÜV SÜD Germany Certification
- Practical Hands-on Training
- Expert Mentors

Cooperation partner of TÜV SÜD

Apply Now!

Contact Us

+91 9846 770 771

18 YEARS OF LEGACY

100% PLACEMENTS ASSISTANCE

100% PRACTICAL TRAINING

INDUSTRY RECOGNIZED CERTIFICATES

Beyond SEO
How AEO is Reshaping The Future of Google Search



MURTHY
DM EXECUTIVE
IPCS GLOBAL MYSORE

For years, finding information online meant typing keywords into Google, scanning search results, and clicking websites to find answers. Search Engine Optimization (SEO) helped businesses improve their visibility and attract relevant visitors.

Today, the search experience is evolving. Google's AI Overviews can summarise information and provide links to relevant sources, while AI Mode supports detailed questions and conversational follow-ups. Instead of simply displaying a list of websites, these features can help users explore topics through AI-generated responses supported by web information.

This transformation has introduced a growing focus on Answer Engine Optimization (AEO). While SEO helps websites become discoverable, AEO emphasises making information clear, relevant, and easy for answer-oriented systems to interpret.

The two approaches are complementary. Businesses that combine strong SEO foundations with useful, well-structured content can prepare for both traditional search and AI-assisted discovery.



1. SEO vs AEO: Understanding the Difference

SEO involves improving a website's visibility, accessibility, and relevance in search engines. It includes keyword research, technical optimisation, internal linking, content quality, and user experience.

AEO focuses more directly on answering users' questions. It encourages content creators to provide clear explanations, address related questions, organise information logically, and support important claims with reliable evidence.

For example, a person searching for a digital marketing course may want to know what the course covers, whether it suits beginners, how long it takes, and which practical skills it teaches.

SEO helps the relevant course page become discoverable. AEO encourages the page to answer these questions clearly.

Area	SEO	AEO
Main focus	Search visibility	Clear, useful answers
Content strategy	Match search intent	Address questions directly
Structure	Relevant pages & internal links	Direct answers & supporting details
Technical	Crawlability & indexability	The same foundations remain important
Requirements Measurement	Rankings, clicks, and conversions	AI visibility where measurable, plus business outcomes

AEO is not a completely separate ranking system. Google continues to recommend established SEO practices for its AI-powered search experiences. The key idea is simple: SEO helps people discover your website, while AEO encourages you to make its information easier to understand and use.



2. How AI Is Changing Search Behaviour

AI-powered search allows users to ask longer, more specific questions in natural language. Instead of performing several separate searches, a user can describe a problem and explore follow-up questions within the same experience.
For instance, someone interested in industrial automation might ask, "Which PLC training course is suitable for beginners and provides practical programming experience?"
Answering this question requires information about course suitability, syllabus, hands-on training, and learning outcomes.

Google's AI Mode can use a technique called query fan-out, which explores related searches to gather information from different angles. Consequently, content that addresses connected questions can be more useful than pages that repeat the same keyword.
This shift creates five important considerations:

Search intent: Solve the user's actual problem instead of focusing only on keywords.
Conversational queries: Address questions people naturally ask.
Topic depth: Include relevant follow-up questions and explanations.
Credibility: Support factual claims with reliable evidence.
Originality: Provide practical examples, expert insights, and information that adds value beyond generic summaries.



3. How to Create Content for SEO and AEO

A successful content strategy does not require abandoning traditional SEO. It requires making content more useful, accurate, and accessible.

Start with real questions : Use customer enquiries, sales conversations, keyword research, and website analytics to understand what your audience wants to know. These questions can become the foundation for articles, tutorials, comparison guides, and FAQs.

Answer questions directly : Introduce the topic and provide a concise explanation near the beginning. Follow it with examples, practical steps, limitations, and supporting information. Readers should not have to search through several paragraphs for the main answer.

Improve readability : Use descriptive headings, short paragraphs, lists, and tables. For technical subjects, diagrams, videos, and relevant images can make complex ideas easier to understand.

Demonstrate expertise : Original research, first-hand experience, expert commentary, and realworld examples help distinguish useful content from generic AI-generated summaries. Accuracy matters: verify statistics, cite credible sources, and update information when necessary.

Maintain technical SEO : Ensure that search engines can crawl and index your pages. Use logical navigation, relevant internal links, mobile-friendly layouts, and appropriate structured data that accurately reflects visible content.

Google states that there are no additional technical requirements specifically for inclusion in AI Overviews or AI Mode beyond normal Google Search eligibility requirements. No special AIonly schema guarantees inclusion.



4. Measuring Success in AI Search

Search performance should not be measured through rankings alone. Businesses need to understand whether their content attracts relevant audiences, satisfies their needs, and contributes to organisational goals.

Performance Area	Key metrics
Visibility	Impressions and search-query coverage
Website traffic	Organic clicks and click-through rate
Engagement	Engaged sessions and relevant interaction metrics
Conversions	Enquiries, registrations, leads, and sales
AI-search presence	Available AI-feature reporting &observable source links

Google Search Console helps website owners monitor search performance. Available reporting for AI features can vary, so marketers should distinguish measured results from estimates. An AI-generated answer may provide useful information without generating a website visit. Therefore, marketers should evaluate both visibility and meaningful business outcomes rather than focusing exclusively on AI mentions.



5. The Future of Search: Preparing for Change

AI is changing how people discover information, but the foundations of successful content remain consistent. Businesses should understand their audiences, publish accurate information, maintain technically sound websites, and demonstrate genuine expertise. They should also avoid shortcuts such as keyword stuffing, mass-producing low-value pages, or relying on unsupported claims about special AI-ranking techniques. For digital marketing professionals, this evolution creates opportunities to develop skills in content strategy, search-intent analysis, technical SEO, analytics, fact-checking, and AI-assisted research. The most effective approach is to treat AEO as an extension of good content strategy rather than a replacement for SEO.

Conclusion: Optimise for People, Prepare for AI

Google Search is evolving towards an experience that combines traditional results with AIgenerated summaries and conversational exploration. SEO remains essential for discoverability, accessibility, and website quality. AEO encourages marketers to organise information around genuine questions and provide clear, well-supported answers. Together, these approaches can help businesses adapt to changing search behaviour while maintaining a strong focus on users.

The goal is not to chase every new optimisation trend. It is to publish content that is accurate, original, easy to navigate, and genuinely useful. The future of search will reward more than the right keywords. It will favour content that helps people understand their questions, evaluate their options, and find trustworthy answers.




SMRITHI T
IT ENGINEER ,
IPCS GLOBAL KOCHI

Zero-Day Attacks: When Cybercriminals Strike before Defenders Can Respond

Imagine discovering that your front door has a serious security flaw. Before you even realise the problem exists, a criminal discovers the weakness and uses it to enter your home. You have no warning, no replacement lock, and no opportunity to secure the entrance before the intrusion. A similar situation can occur in cybersecurity when attackers discover and exploit a previously unknown software or hardware vulnerability. Known as zero-day vulnerability, this type of security flaw can leave organizations exposed before an effective fix becomes available. Attackers may exploit the weakness to access sensitive
information, compromise devices, or establish unauthorized access to critical systems. The term zero-day refers to the lack of preparation time available to defenders before exploitation or remediation becomes possible. Such vulnerabilities are particularly challenging because traditional security measures may not recognize an attack that uses a previously unknown technique.



However, zero-day attacks are not impossible to defend against. Although organisations may be unable to patch a flaw before its discovery, they can reduce their exposure through layered security, behavioral monitoring, rapid incident response, and effective vulnerability management.

What Is Zero-Day Vulnerability?

Vulnerability is a weakness in software, hardware, firmware, or system configuration that an attacker may exploit to compromise security.

Zero-day vulnerability is generally understood as a previously unknown security flaw for which an effective fix is not yet available to the affected organization or users. The precise terminology can vary depending on whether the weakness is known to the vendor, publicly disclosed, or already being exploited.

Consider a web browser containing an undiscovered memory-handling flaw. An attacker finds away to use specially crafted content to trigger unintended behaviour.

At this stage, the software may still appear to function normally. The vendor may not know about the flaw, security teams may have no specific detection rule for it, and an official patch may not exist.

If an attacker successfully uses the vulnerability against a target before effective remediation is available, the incident may constitute a zero-day attack.

The key concern is the gap between the existence of a vulnerability and the ability of defenders to address it.

Vulnerability, Exploit, and Attack: Understanding the Difference

These three terms are closely related, but each describes a different part of the threat.

Zero-day vulnerability: The underlying security weakness.

Zero-day exploit: The technique or code used to take advantage of that weakness.

Zero-day attack: The real-world attempt to exploit the weakness against a target.

For example, a previously unknown browser flaw is the vulnerability. A specially crafted webpage designed to trigger that flaw represents the exploit mechanism. When an attacker uses it to compromise a victim's device, the event becomes an attack. Understanding these differences helps cybersecurity teams investigate incidents, communicate risks, and select appropriate defensive measures.

Why Are Zero-Day Attacks So Dangerous?

The primary challenge is that defenders may have limited information about the vulnerability and how it is being exploited.



No immediate patch may exist. If the vendor has not identified the flaw, users may have no official security update to install. Other protective measures must help reduce the risk until a fix becomes available.

Traditional detection may be less effective. Signature-based security tools often rely on known malicious files or previously identified attack patterns. An unfamiliar exploit may bypass some of these controls, although modern security products can also use behavioural and anomaly detection.

High-value systems may be targeted. Government agencies, financial institutions, technology companies, telecommunications providers, and critical infrastructure operators may be attractive targets because of the information or access they hold.

Attackers may exploit the flaw before public disclosure. Vulnerabilities can be discovered independently by researchers or threat actors. Some may also be traded privately, meaning defenders cannot assume that an unknown vulnerability is not already being exploited.

These factors make zero-days difficult to manage. The absence of a known flaw does not mean a system is secure.



How Does a Zero-Day Attack Unfold?

Although attacks differ considerably, a typical incident may involve several stages

1. Vulnerability discovery

A researcher, developer, or attacker identifies a weakness in software, hardware, or firmware. Responsible disclosure may allow the vendor to investigate and prepare a fix before criminals exploit the issue.

2. Exploit development

An attacker develops a method to trigger the vulnerability. Depending on the flaw, exploitation might enable unauthorized code execution, privilege escalation, information theft, or securitycontrol bypass.

3. Delivery

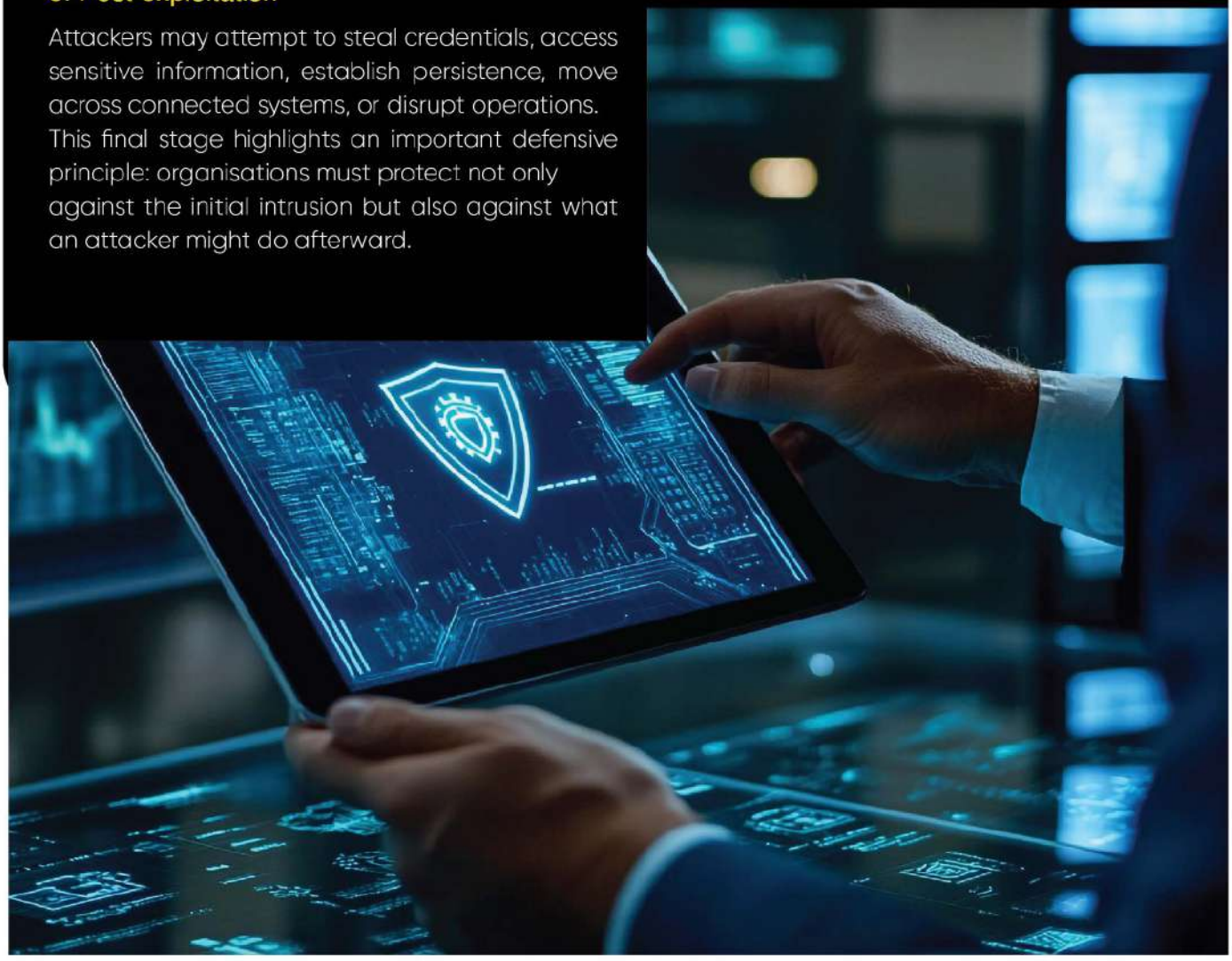
The attacker attempts to reach the target through a possible entry point, such as a malicious website, phishing message, compromised service, or vulnerable internet-facing device. Some attacks combine multiple vulnerabilities into an exploit chain.

4. Exploitation

If the attack succeeds, the vulnerable component behaves in an unintended way. Initial access does not necessarily provide complete control; additional weaknesses may need to be exploited.

5. Post-exploitation

Attackers may attempt to steal credentials, access sensitive information, establish persistence, move across connected systems, or disrupt operations. This final stage highlights an important defensive principle: organisations must protect not only against the initial intrusion but also against what an attacker might do afterward.



Where Can Zero-Day Vulnerabilities Occur?

Almost any technology containing software or programmable components can be affected

Operating systems: Vulnerabilities can affect Windows, Linux, macOS, Android, and other platforms.

Web browsers: Browsers process large amounts of untrusted internet content, making their security particularly important.

Mobile devices: Operating systems, applications, and communication components can introduce security weaknesses.

Network appliances: Routers, firewalls, and VPN gateways may provide valuable entry points when exposed to external networks.

Enterprise applications: Email platforms, identity systems, collaboration tools, and business applications can hold sensitive organisational data.

IoT and embedded systems: Cameras, smart appliances, medical devices, and industrial equipment may contain vulnerabilities that are difficult to identify or patch quickly.

In industrial environments, the consequences can extend beyond data theft. A compromised control system may affect production availability, process integrity, or operational safety. Industrial control systems therefore require security measures that account for both cybersecurity and physical-process requirements.



Zero-Day vs. Known Vulnerabilities

Zero-day vulnerability	Known vulnerability
Not yet known to defenders or not effectively addressed	Identified and documented
An effective patch may not be available	A patch or mitigation may be available
Detection may require behavioral analysis and investigation	Existing security tools may recognize known indicators
Defenders may have little warning	Organizations may have an opportunity to respond
Requires layered protection and rapid response	Prioritized patching is often a key mitigation

A known vulnerability can still be extremely dangerous if an organization fails to patch it. In many incidents, attackers succeed not because a flaw is unknown, but because an available security update was never installed.

Building a Practical Zero-Day Defense Strategy

No single tool can guarantee protection against every zero-day attack. A more effective approach combines several complementary measures.

Reduce the attack surface. Disable unnecessary services, remove unused applications, restrict internet exposure, and review access permissions regularly.

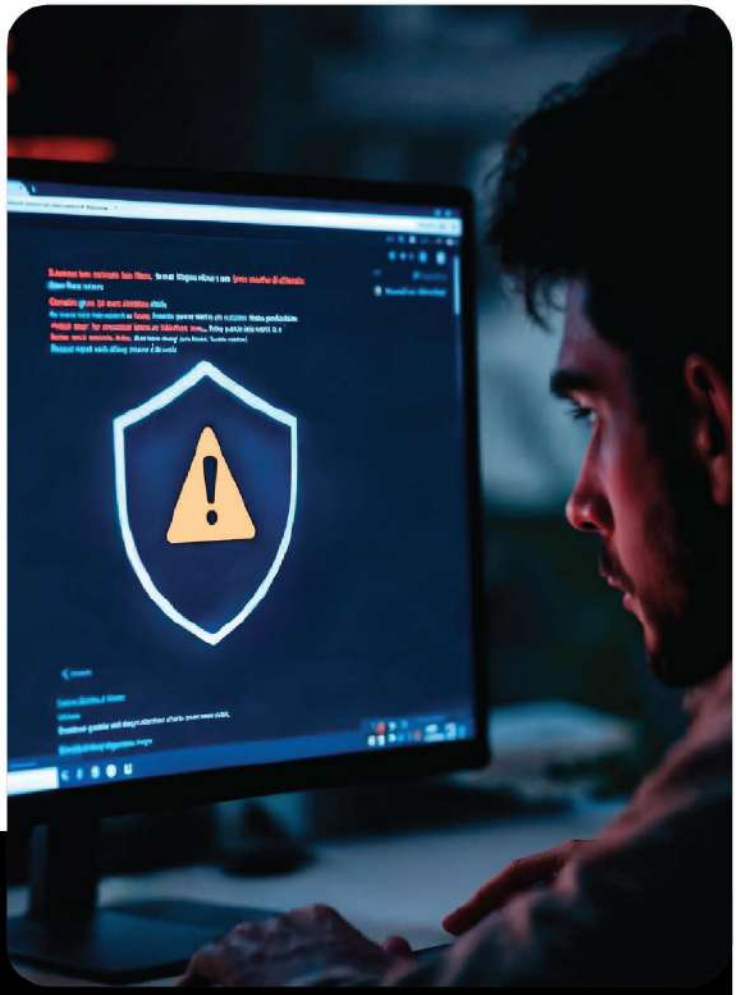
Use defense in depth. Combine endpoint protection, network segmentation, multi-factor authentication, least-privilege access, and secure configurations so that one failed control does not automatically compromise the entire environment.

Monitor behavior. Use endpoint detection and response (EDR), network monitoring, centralized security logging, and security information and event management (SIEM) systems to identify suspicious activity, including behavior that does not match known attack signatures.

Prepare for incidents. Establish an incident response plan covering detection, containment, investigation, communication, recovery, and evidence preservation. Test the plan through exercises rather than relying solely on written procedures.

Patch according to risk. When a vendor releases an update for an actively exploited vulnerability, prioritize deployment according to exposure, criticality, and operational requirements. Where immediate patching is not feasible, apply suitable vendor-recommended mitigations and monitor the affected systems closely.

Secure applications from development onward. Secure coding practices, code reviews, testing, and vulnerability disclosure programmers can help identify weaknesses before attackers discover them.



Conclusion: Preparation Is the Strongest Defense

Zero-day vulnerabilities represent a difficult challenge because attackers may gain an advantage before defenders understand the weakness or receive an effective patch. Their impact can extend across personal devices, enterprise applications, cloud services, network infrastructure, and industrial control systems. Yet effective cybersecurity is not about finding one perfect security tool. It is about building a resilient environment that can prevent many attacks, recognize suspicious behavior, contain compromises, and recover quickly.

Organizations should combine secure development, vulnerability management, endpoint protection, identity security, network segmentation, threat intelligence, monitoring, reliable backups, and tested incident response procedures. They should also pay close attention to known vulnerabilities that remain unpatched, since these can be just as damaging. As artificial intelligence, cloud computing, and connected technologies continue to evolve, both attackers and defenders will gain new capabilities. The challenge for organizations will be to adapt their security practices without losing sight of the fundamentals.

A zero-day may give an attacker an unexpected opening, but strong preparation, layered defenses, and a rapid response can prevent that opening from becoming a major security incident.

Winning Attention without Losing Trust:

The Human Equation in Digital Marketing



NANDANA
CRE, IPCS GLOBAL TRIVANDRUM

A social media advertisement appears just after you search for a product. An influencer recommends a new brand, and a few minutes later, you find the same product promoted across several platforms. These everyday experiences reveal how deeply digital marketing has become part of our lives.

Businesses today have more ways than ever to reach potential customers. Search engine optimization (SEO), social media campaigns, email marketing, influencer partnerships, and artificial intelligence (AI) help brands connect with people, understand their preferences, and deliver personalized messages.

But this growing ability to influence consumer decisions comes with responsibility. How much personal information should businesses collect? When does persuasive advertising become misleading? Should customers always know when an influencer is being paid to promote a product?

These questions lie at the heart of digital marketing ethics. In an environment where information travels quickly and public opinion can change overnight, businesses need more than effective campaigns. They need practices that respect consumers and earn their trust.

What Does Ethical Digital Marketing Mean?

Ethical digital marketing is the practice of promoting products and services through honesty, fairness, transparency, and respect for consumer rights. It involves making responsible choices at every stage of a campaign, from collecting customer information to creating advertisements and measuring results. Ethical marketers avoidmisleading claims, protect personal data, disclose commercial relationships, and give consumers meaningful control over their choices.Following the law is an essential starting point, but ethical responsibility goes further. A marketing practice may be technically permissible and still leave customers feeling manipulated or misled. Today's consumers can compare prices, research brands, read reviews, and share their experiences with a global audience. A misleading advertisement or careless approach to customer data can quickly damage a reputation that took years to build.

For this reason, ethical marketing is not simply a matter of avoiding complaints. It is about creating relationships in which customers feel informed, respected, and confident in their decisions.

Why Trust Matters More Than Ever

A successful marketing campaign may generate thousands of clicks, views, and enquiries. But these numbers mean little if customers do not trust the brand behind them.

Trust influences whether people return to a business, recommend its products, or continue buying from it when competitors offer attractive alternatives. It also shapes how customers respond when a company makes a mistake.

Ethical marketing supports long-term business growth in several ways:

Stronger brand reputation: Honest communication helps build a positive and credible public image.

Customer loyalty: People are more likely to maintain relationships with brands that respect their interests.

Better customer experiences: Clear information and responsible personalisation help customers make informed choices.

Positive word of mouth: Satisfied customers can become genuine advocates for a business.

Lower compliance risks: Responsible practices can reduce the likelihood of privacy violations and misleading advertising claims.

Sustainable growth: Building relationships around trust creates a stronger foundation than relying on short-term attention alone.

Unethical practices may produce quick results, but the long-term costs can be substantial. Lost customers, public criticism, regulatory consequences, and damaged credibility can outweigh the immediate benefits of a successful campaign.



The Ethical Challenges behind the Screen

Digital marketing continues to evolve, and each new tool introduces questions about how it should be used. Some of the most important challenges concern privacy, advertising transparency, online reviews, influencer promotions, and AI-generated content.

1. Data Privacy: Knowing Where to Draw the Line

Personal data plays a major role in modern marketing. Businesses may use browsing activity, purchase history, location information, and stated preferences to understand customer behaviour and deliver relevant advertisements.When handled responsibly, this information can improve the customer experience. However, collecting more data than necessary, using it for purposes customers did not expect, or failing to protect it can undermine consumer confidence.

Responsible marketers should explain what information they collect, why they need it, and how they intend to use it. They should obtain consent where required, secure stored information, limit access to authorised personnel, and provide appropriate ways for users to exercise their privacy rights.The guiding principle is straight forward: just because a business can collect information does not mean it should collect or use it without careful consideration.



2. Honest Advertising: Promises Must Match Reality

Advertising is designed to attract attention and persuade people to take action. The ethical problem begins when persuasion depends on false promises or deliberately misleading information.

Exaggerated product claims, fake discounts, hidden charges, manipulated images, and unclear terms can create expectations that a product or service cannot fulfil.

For example, advertising a product as being available at a special price is misleading if the original price has been artificially inflated to make the discount appear more impressive.

Ethical advertising requires businesses to present accurate information, explain important conditions clearly, substantiate factual claims, and ensure that the overall message does not create a false impression.

Creative communication and persuasive storytelling have their place in marketing. Deception should not.

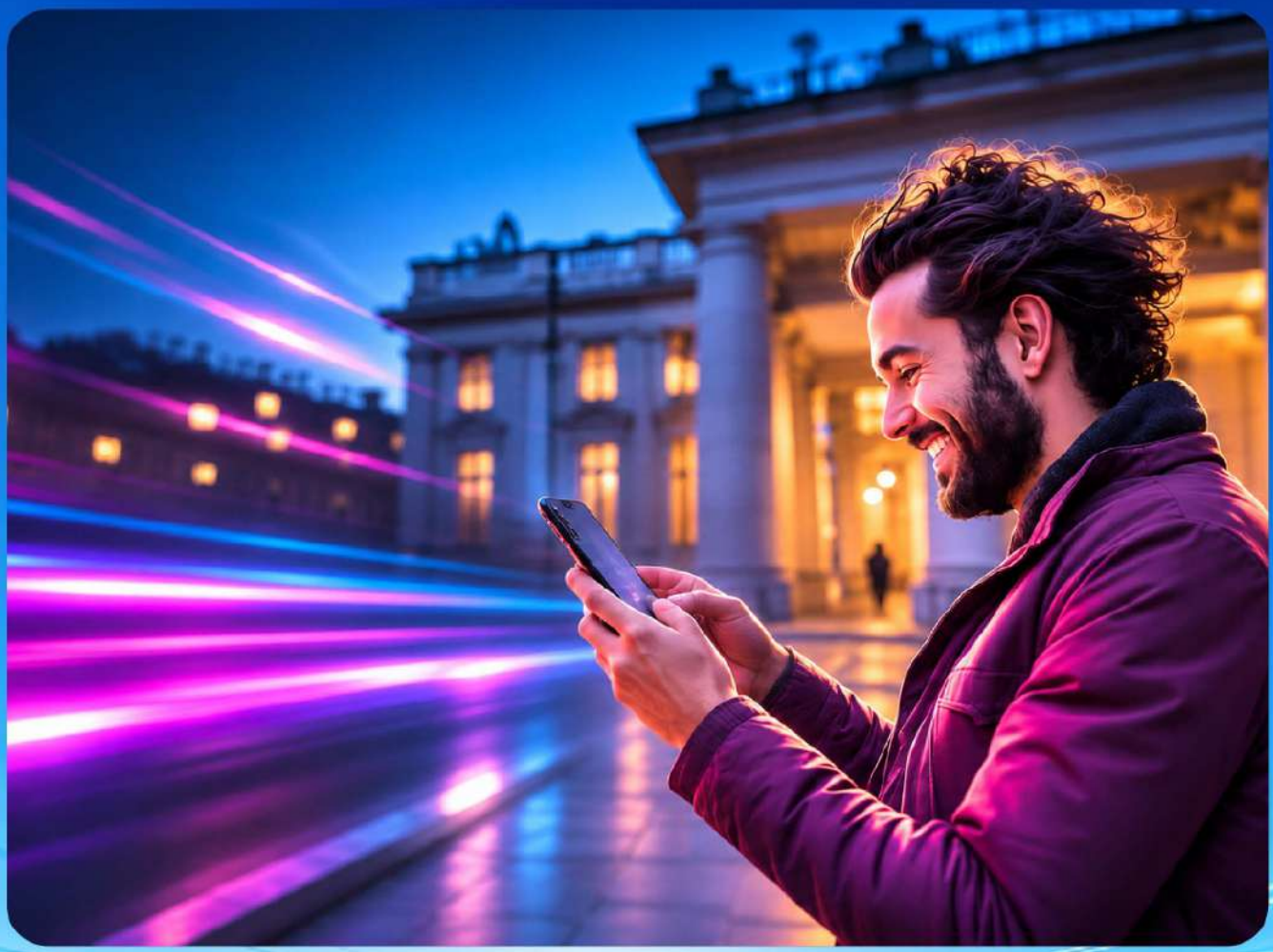
3. Influencer Marketing: Making Paid Partnerships Clear

Influencers can shape purchasing decisions because their audiences often view them as relatable and trustworthy. Brands benefit from these relationships by reaching communities that traditional advertisements may struggle to engage.

However, the relationship becomes questionable when paid promotions are presented as entirely independent opinions. If an influencer receives payment, free products, commissions, or other benefits in exchange for promotional content, the commercial relationship should be disclosed clearly and prominently, in accordance with applicable rules.

Influencers should also be honest about their experiences and avoid making unsupported claims about a product's performance or benefits.

A genuine recommendation can be valuable to both the audience and the brand. Concealing the commercial relationship risks damaging the very trust that makes influencer marketing effective.





4. Fake Reviews: When Social Proof Becomes Deception

Before buying a product, many customers check online ratings and reviews. These opinions can help people understand product quality, customer service, and potential limitations.

Fake reviews distort this process. Some businesses publish fabricated positive feedback to improve their ratings, while others attempt to damage competitors through dishonest negative reviews.

Such practices mislead customers and create an unfair competitive environment.

Businesses should encourage genuine feedback, avoid purchasing fabricated reviews, and respond constructively to criticism. Negative reviews should not automatically be treated as a threat; they can reveal problems that need attention and opportunities to improve.

Authentic feedback may not always be flattering, but it is far more valuable than a reputation built on false impressions.

5. Clickbait: Winning the Click but Losing the Reader

A headline such as "You Won't Believe What Happens Next" may attract attention, but what happens when the article fails to deliver on its promise?

Clickbait uses sensational or misleading headlines to generate clicks, often at the expense of accuracy and reader satisfaction. Although it can increase traffic in the short term, repeated disappointment can make audiences less willing to trust future content.

Effective marketing does not require every headline to be dramatic. A strong headline should create curiosity while accurately reflecting the content that follows.

The goal should be to attract the right audience and provide genuine value, not simply to increase the number of clicks.

6. Artificial Intelligence: Efficiency With Accountability

AI is changing the way marketers work. It can help generate content ideas, analyse customer behaviour, personalise campaigns, power chatbots, and automate repetitive tasks.

These capabilities offer significant advantages, but they also introduce ethical concerns.

AI-generated content may contain inaccurate information, reproduce biases present in training data, or create messages that unfairly influence particular audiences. Automated targeting can also raise concerns when sensitive personal characteristics are involved.

Human oversight remains important. Marketing teams should verify factual claims, assess potential bias, protect customer information, and take responsibility for the content and decisions produced with AI assistance. The objective is not to avoid AI. It is to use the technology in ways that improve marketing without compromising accuracy, fairness, or consumer trust.





Responsible Communication on Social Media and Email

Social media and email remain two important channels for building customer relationships. Both offer businesses direct access to audiences, but they also demand respect for people's time,preferences, and personal boundaries.

On social media, ethical marketing means sharing accurate information, moderating discussions responsibly, avoiding discriminatory or offensive messaging, and responding professionally to customer concerns. Engagement should come from meaningful interaction rather than manufactured controversy or manipulative tactics. Email marketing requires similar care. Businesses should follow applicable consent and privacy requirements, send relevant content, explain why recipients are receiving messages, and provide a clear, easy way to unsubscribe. Sending repeated messages to people who have withdrawn their permission or using confusing subscription practices may increase short-term exposure, but it can also create frustration and damage the brand's reputation. Respectful communication recognises that customers are people with choices, not simply numbers on a marketing dashboard.

Corporate Social Responsibility: Values Must Be Genuine

Consumers increasingly pay attention to how businesses behave beyond the products they sell.

Environmental sustainability, diversity, inclusion, fair working practices, and community development can all influence how people view a brand.

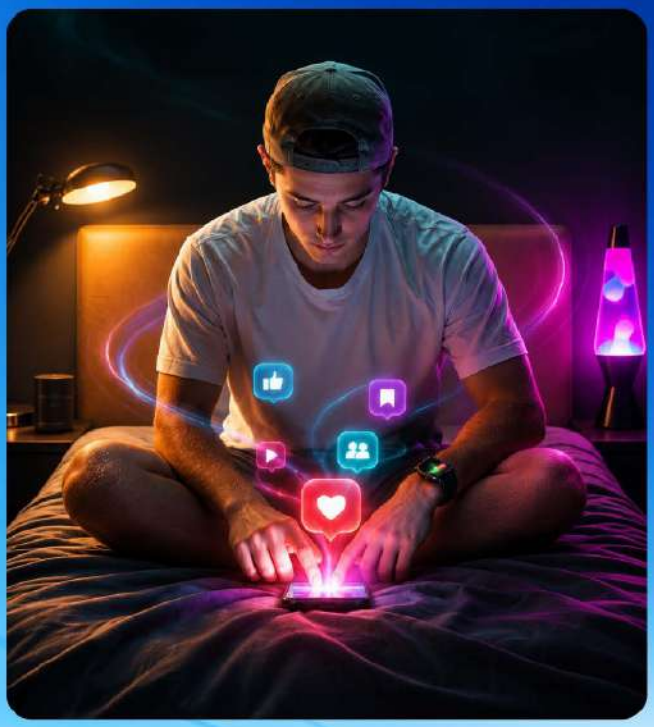
Corporate social responsibility (CSR) gives businesses an opportunity to demonstrate their commitment to wider social and environmental concerns. Digital marketing can help communicate these efforts, share progress, and encourage public participation.

However, the message must reflect reality. However, the message must reflect reality.

A company that promotes environmental responsibility without meaningful action risks accusations of greenwashing. Similarly, using social causes purely to attract attention, without a genuine commitment to the issue, can weaken public trust.

Responsible marketing should communicate real initiatives honestly, acknowledge limitations, and support claims with evidence wherever possible.

A brand's values become credible when its actions consistently support its words



Turning Ethical Principles Into Everyday Practice

Ethical marketing becomes meaningful when it is reflected in routine business decisions rather than treated as a statement of intent. Organisations can strengthen their approach by following several practical principles:

Communicate clearly: Make product information, pricing, limitations, and important terms easy to understand.

Protect personal information: Collect only what is necessary, apply appropriate security measures, and respect privacy rights.

Be transparent: Clearly identify sponsored content and disclose relevant commercial relationships.

Verify before publishing: Check facts, statistics, product claims, and AI-generated material

Avoid manipulative design: Do not use confusing interfaces, hidden conditions, or coercive tactics to pressure customers into decisions.

Respect customer choices: Make consent, subscription preferences, and withdrawal options straightforward.

Train marketing teams: Help employees understand evolving privacy expectations, advertising standards, platform policies, and responsible AI use.

Measure more than clicks: Consider customer satisfaction, complaint rates, repeat business, and long-term trust alongside campaign performance.

These practices help bring ethical principles into campaign planning, content creation, advertising, analytics, and customer service.

Conclusion: Trust Is the Real Measure of Success

Digital marketing will continue to change as AI, automation, analytics, and new communication platforms reshape the way businesses reach people. These technologies will create fresh opportunities, but they will also demand greater care in how information is collected, messages are presented, and customer decisions are influenced.

The most effective marketing is not necessarily the marketing that attracts the most attention. It is the marketing that delivers genuine value without misleading or exploiting its audience.

For students entering the industry, ethical awareness should be part of developing strong marketing skills. For professionals and business leaders, it should guide the decisions behind every campaign.

Clicks can be counted, impressions can be measured, and conversions can be tracked. Trust, however, is earned through consistent action.

In the long run, responsible digital marketing succeeds not just by persuading people to buy, but by giving them good reasons to believe in the brand.



The Future of BMS: Autonomous & Smart Buildings



AKHILESH
PROJECT ENGINEER,
IPCS GLOBAL CALICUT



DEVANAND
BMS ENGINEER,
IPCS GLOBAL CALICUT

Building Management Systems (BMS) are entering a new era. Traditionally, they have been used to monitor and control HVAC, lighting, electrical equipment, pumps, and other building services. In the coming years, advances in artificial intelligence, the Internet of Things (IoT), digital twins, robotics, and intelligent energy management could transform BMS from monitoring platforms into systems that actively predict needs and optimise building performance.

1. Artificial Intelligence: Buildings That Learn and Adapt

One of the most promising developments in BMS is the integration of artificial intelligence (AI) and machine learning. Traditional control systems generally operate according to programmed logic,
fixed schedules, and predefined setpoints.
AI-enabled systems could analyse historical and real-time
data to identify patterns and recommend more effective operating strategies.
For example, an intelligent HVAC system could learn how temperature changes throughout the day,
how occupancy affects cooling demand, and how weather conditions influence energy consumption.
It could then recommend adjustments to cooling schedules while maintaining required comfort conditions.

The future building will not simply respond to commands or predefined schedules. It will increasingly learn from operational data, anticipate equipment problems, adapt to occupancy, and coordinate energy consumption with external power systems. These developments could redefine the responsibilities of BMS engineers and the way commercial buildings, hospitals, airports, hotels, and industrial facilities are managed.

AI could also improve alarm management by distinguishing recurring minor issues from patterns
that indicate developing equipment failures. Instead of presenting operators with hundreds of unrelated notifications, future systems may prioritise the alarms that require immediate attention.
However, AI recommendations will still need suitable validation, reliable sensor data, and engineering oversight, particularly where safety and critical building operations are involved.



2. Predictive Maintenance: Detecting Problems Before Failure

Future BMS platforms are likely to make greater use of predictive and condition-based maintenance. Rather than depending only on fixed maintenance schedules or waiting for equipment to fail, these systems will increasingly analyse equipment performance to identify early warning signs.

Sensors monitoring vibration, temperature, pressure, electrical consumption, and operating cycles can provide information about motors, pumps, chillers, cooling towers, and air-handling units.

Machine-learning models may use these measurements to identify unusual behaviour, such as a gradual increase in motor vibration or a chiller consuming more electricity than expected for its cooling output.

Maintenance teams could receive an early warning before a fault develops into an expensive breakdown.

Digital maintenance records could also help estimate the urgency of repairs and prioritise service activities.

As these capabilities mature, BMS engineers may spend less time responding to unexpected faults and more time analysing equipment performance, validating predictions, and planning preventive interventions.





3. Digital Twins: Creating Virtual Buildings

A digital twin is a digital representation of a physical building, its equipment, and its operating conditions. When connected to live BMS data, it can help facility teams understand how the real building behaves and explore possible changes before implementing them. Imagine a large commercial building preparing to expand its office space. A digital twin could help engineers examine how the proposed occupancy might affect cooling loads, ventilation requirements, energy consumption, and equipment capacity.



Digital twins could also support commissioning, troubleshooting, and energy optimisation by comparing expected performance with actual operating data.

In the future, combining digital twins with AI may enable more sophisticated simulations of building operations. Engineers could test alternative schedules, evaluate equipment upgrades, and investigate potential faults in a virtual environment before changing the physical system.

This technology could make building design, commissioning, and long-term maintenance more data-driven.







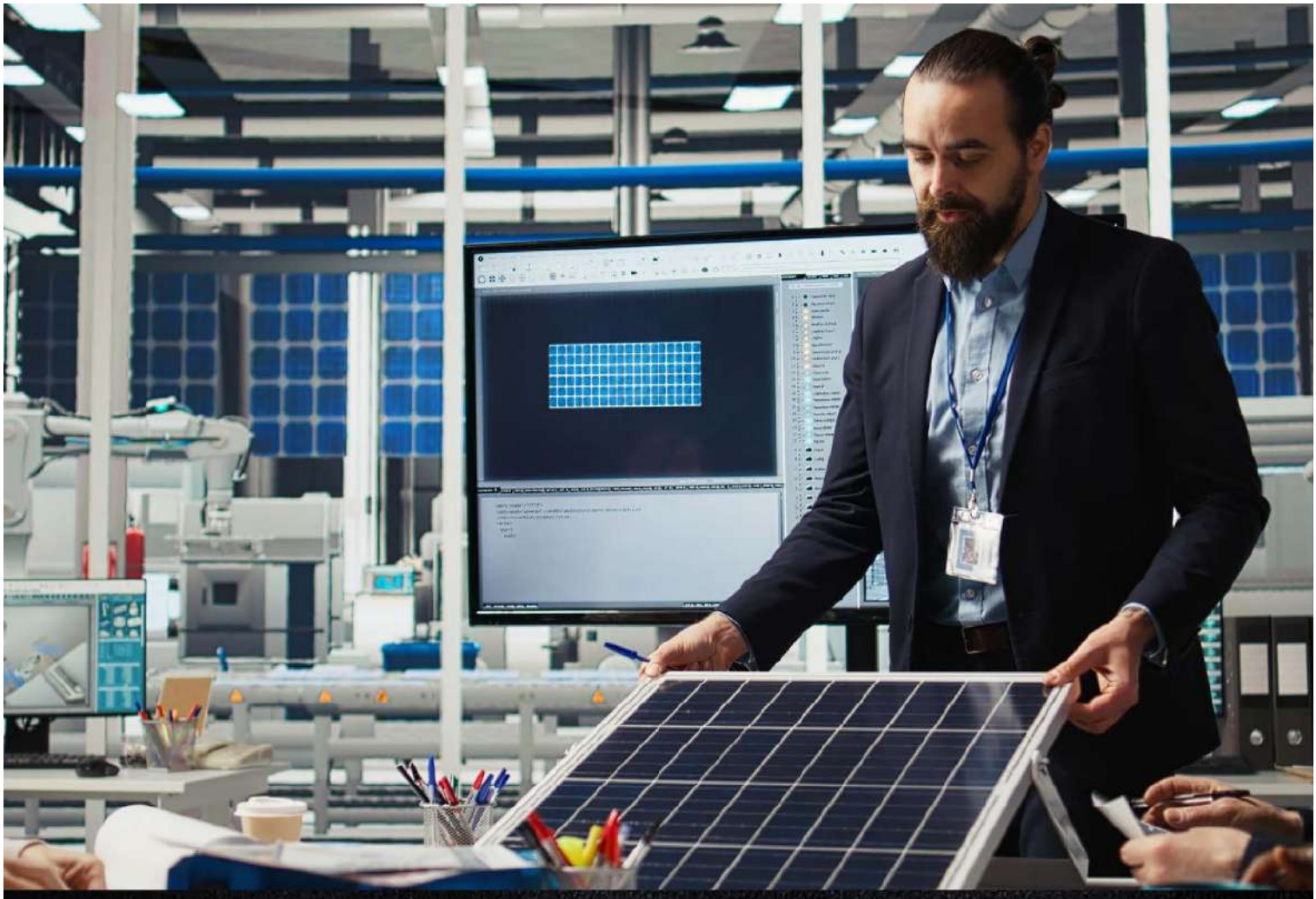
4. AutonomOus Buildings and Intelligent Occupancy Management

Future buildings may become increasingly responsive to the people using them. Connected occupancy sensors, indoor positioning technologies, and environmental monitoring systems could help BMS platforms understand how spaces are being used.

For example, an intelligent office building could adjust lighting and ventilation according to actual occupancy rather than relying entirely on fixed schedules. Meeting rooms could prepare themselves for expected use, while unused areas could operate in energy-saving modes where appropriate.

Hospitals, airports, hotels, and shopping centres could benefit from more dynamic control of indoor conditions because occupancy patterns often change throughout the day. Advanced systems may also coordinate multiple building services instead of controlling each independently. HVAC, lighting, blinds, and ventilation could work together to balance comfort, energy use, and indoor air quality.

The goal is not simply to automate more equipment. It is to create environments that respond intelligently to changing conditions without compromising occupant comfort, privacy, or safety.



5. Smart Energy Management and Grid Integration

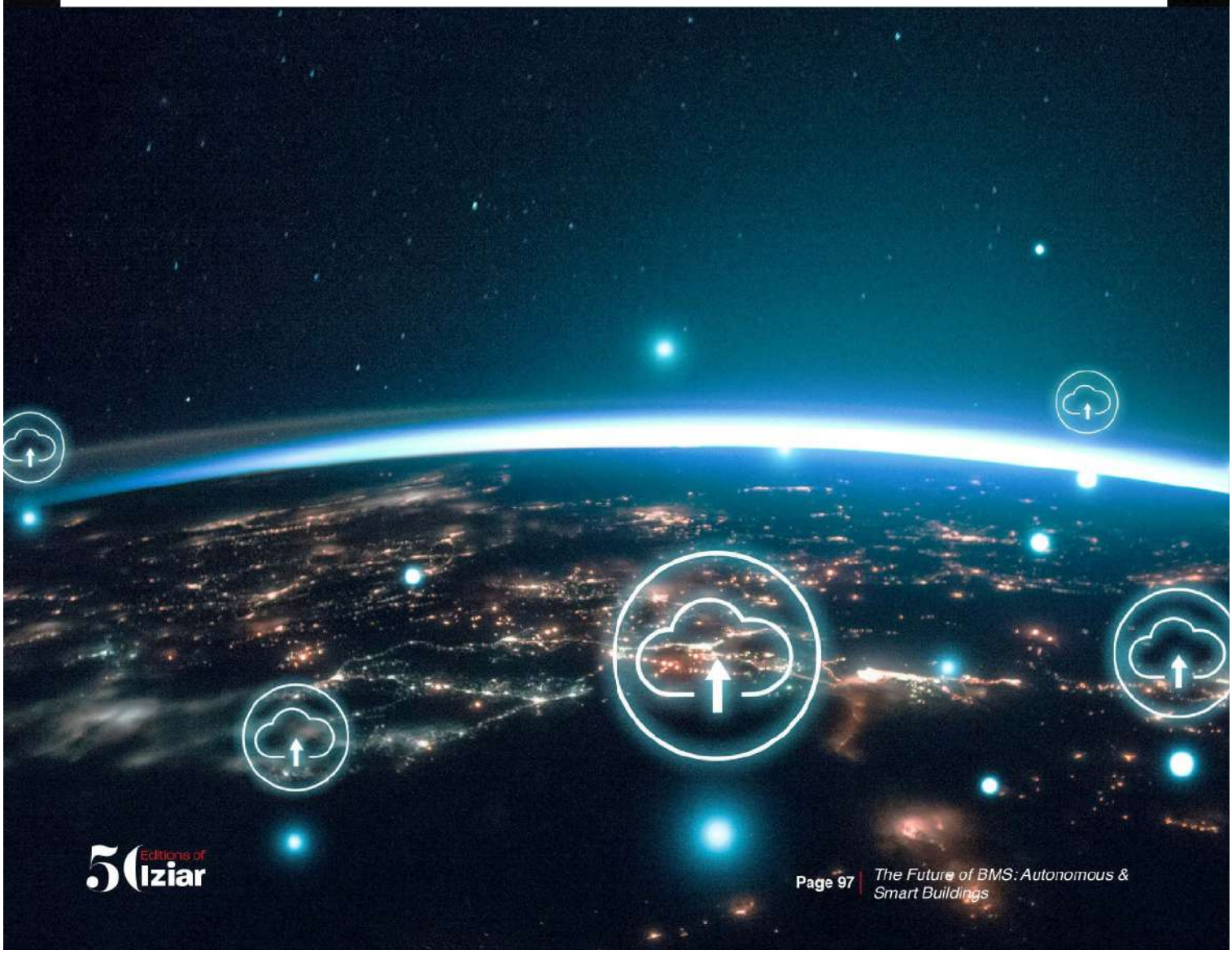
Energy management will become increasingly important as buildings adopt renewable energy, battery storage, electric vehicle charging, and smarter electricity networks. Future BMS platforms could coordinate these resources according to building demand, energy prices, weather forecasts, and electricity-grid conditions. For instance, a building with rooftop solar panels and battery storage might use available solar power during the day, store excess energy when appropriate, and reduce consumption during periods of high electricity demand.

Advanced systems could also support demand response, adjusting selected non-critical loads when the electricity grid requires flexibility. AI-assisted optimisation may help facility managers compare different operating strategies while respecting equipment limits and occupant electrical loads intelligently.

Instead of allowing every charging station to draw maximum power simultaneously, the system could distribute available capacity according to building demand and charging priorities. These developments could turn BMS into a key part of the future energy ecosystem.

6. Edge Computing, Cloud Platforms, and Connected Buildings

The future of BMS will likely combine local processing with cloud-based analytics. Edge computing allows controllers and gateways to process information close to the equipment, reducing communication delays and supporting local operation when external connectivity is unavailable. Cloud platforms, meanwhile, can provide greater computing capacity for historical analysis, portfolio-wide performance comparisons, and advanced AI applications. A facility manager responsible for multiple buildings could compare energy consumption, equipment efficiency, and maintenance trends from a central dashboard. Remote experts could also help investigate faults without always travelling to the site. However, cloud connectivity should not become a single point of failure. Essential control functions must continue locally whenever required, and remote access must be protected through strong authentication, appropriate permissions, network segmentation, and secure updates.



7. Robotics and Autonomous Facility Operations

Robotics could become another important element of smart building management. Autonomous robots may support routine inspections, security patrols, delivery tasks, and selected maintenance activities.

When connected to building information systems, these robots could receive information about access permissions, floor conditions, equipment locations, and designated routes.

For example, a mobile inspection robot could capture thermal images of selected electrical equipment or check environmental conditions in designated areas. The collected data could then be reviewed alongside BMS alarms and maintenance records.

Although widespread autonomous maintenance remains a developing possibility, integration between robotics and building systems could eventually reduce repetitive work and help personnel inspect difficult-to-access areas more efficiently.

Human supervision will remain important for interpreting results, managing unusual situations, and carrying out repairs that require technical judgement.





8. The Future Role of BMS Engineers

As BMS technology evolves, the skills required of engineers will expand beyond conventional controller programming and HVAC troubleshooting.

Future professionals may need working knowledge of AI-assisted analytics, IoT communication, BACnet and Modbus integration, cloud platforms, cybersecurity, energy management, and digital-twin technologies.

Data interpretation will become especially valuable. Engineers will need to distinguish genuine equipment faults from inaccurate sensor readings, assess automated recommendations, and ensure that optimisation strategies follow operational and safety requirements.

Cybersecurity will also remain a critical responsibility as more building systems become connected.

Protecting controllers, engineering workstations, networks, and remote-access services will be essential to reliable building operation.

For aspiring BMS professionals, learning traditional control fundamentals alongside networking, analytics, and emerging automation technologies will provide a strong foundation for the next generation of smart buildings.



Conclusion: Building an Intelligent Future

The future of Building Management Systems extends far beyond centralised monitoring. AI, predictive maintenance, digital twins, autonomous control, smart energy management, and robotics could make buildings more adaptive, efficient, and responsive. These technologies will not eliminate the need for experienced engineers. Instead, they will change how engineers design systems, diagnose problems, manage energy, and maintain building performance.

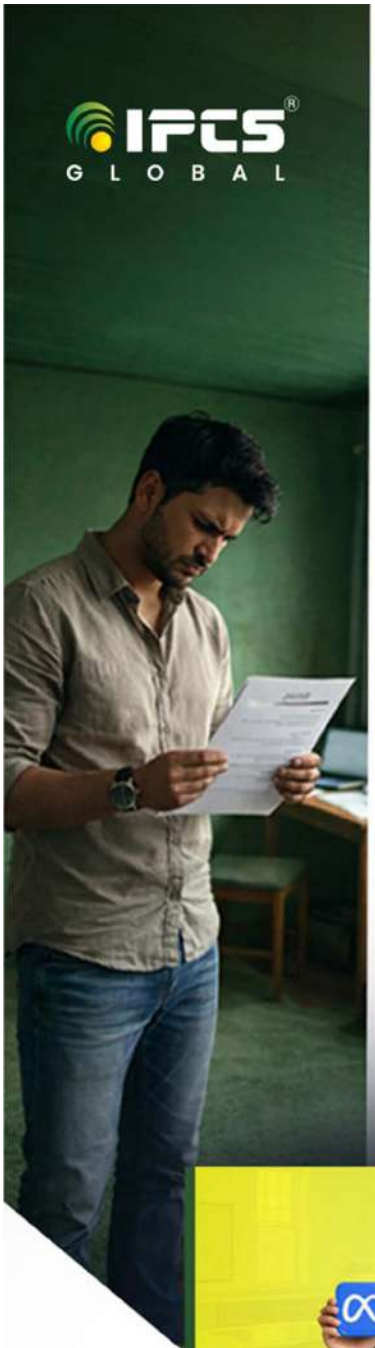
The next generation of BMS will depend on combining intelligent software with reliable field devices, sound engineering principles, cybersecurity, and human oversight.

The future building will not merely be automated. It will increasingly be predictive, connected, energy-aware, and capable of adapting to the people and environments it serves.

IFCS GLOBAL

www.ipcsglobal.com

BECOME AN AI- INTEGRATED DIGITAL MARKETING EXPERT!





WITH A **HIGH SALARY** AND GLOBAL DEMAND!

1200+ SUCCESSFULL Placements In 2025

IFCS GLOBAL

Learn

The Digital Marketing Skills Companies are Hiring for

- *100% Placement Assistance*
- *Practical Learning with Live Projects*
- *One-to-One Mentorship & Career Guidance*
- *Industry-Relevant Latest Curriculum*

Enquire Now



POORNAMANIKANDAN M
DM EXECUTIVE,
IPCS GLOBAL TIRUNELVELI

The Next Click:
Redefining Digital Marketing

For years, digital marketing followed a familiar path: rank on Google, attract website visitors, generate leads, and convert them into customers. In 2026, that journey is changing rapidly.

Search engines are delivering direct answers, advertising platforms are relying more heavily on artificial intelligence, and privacy regulations are changing how businesses collect data and measure success.

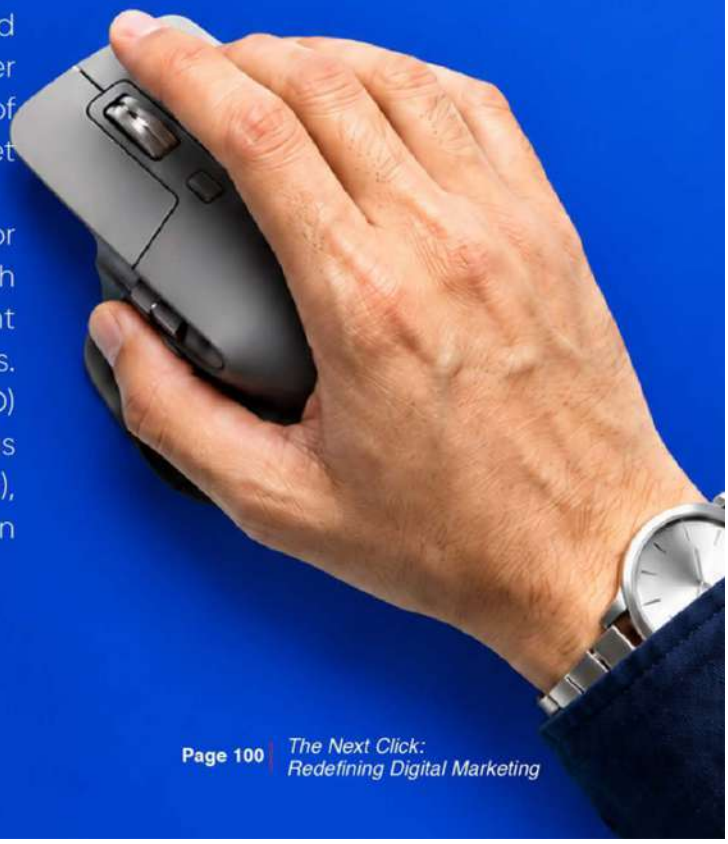
Today, digital marketers face a bigger challenge than simply attracting traffic. They must understand where customers discover information, how they make decisions, and what it takes for a brand to earn their trust across an increasingly AI-driven digital landscape.

Search Is Evolving from Results to Answers

People are no longer relying exclusively on traditional search results to find information.

Google's AI Overviews and AI Mode, along with platforms such as ChatGPT, Perplexity, and Gemini, are changing how users discover products, services, and solutions. Instead of visiting multiple websites, users can often get answers directly from AI-powered tools.

This shift creates a new challenge for businesses. A website may rank well in search results but still miss opportunities if its content is not referenced in AI-generated answers. Traditional Search Engine Optimisation (SEO) remains important, but brands must also focus on Generative Engine Optimisation (GEO), which aims to improve their visibility in AI-generated responses.



Businesses can adapt by publishing clear, reliable, and useful content that directly answers customer questions. Sharing original research, practical examples, customer case studies, and accurate business information can strengthen credibility. Structured data and consistent business details across websites and online directories can also help search systems understand the brand.

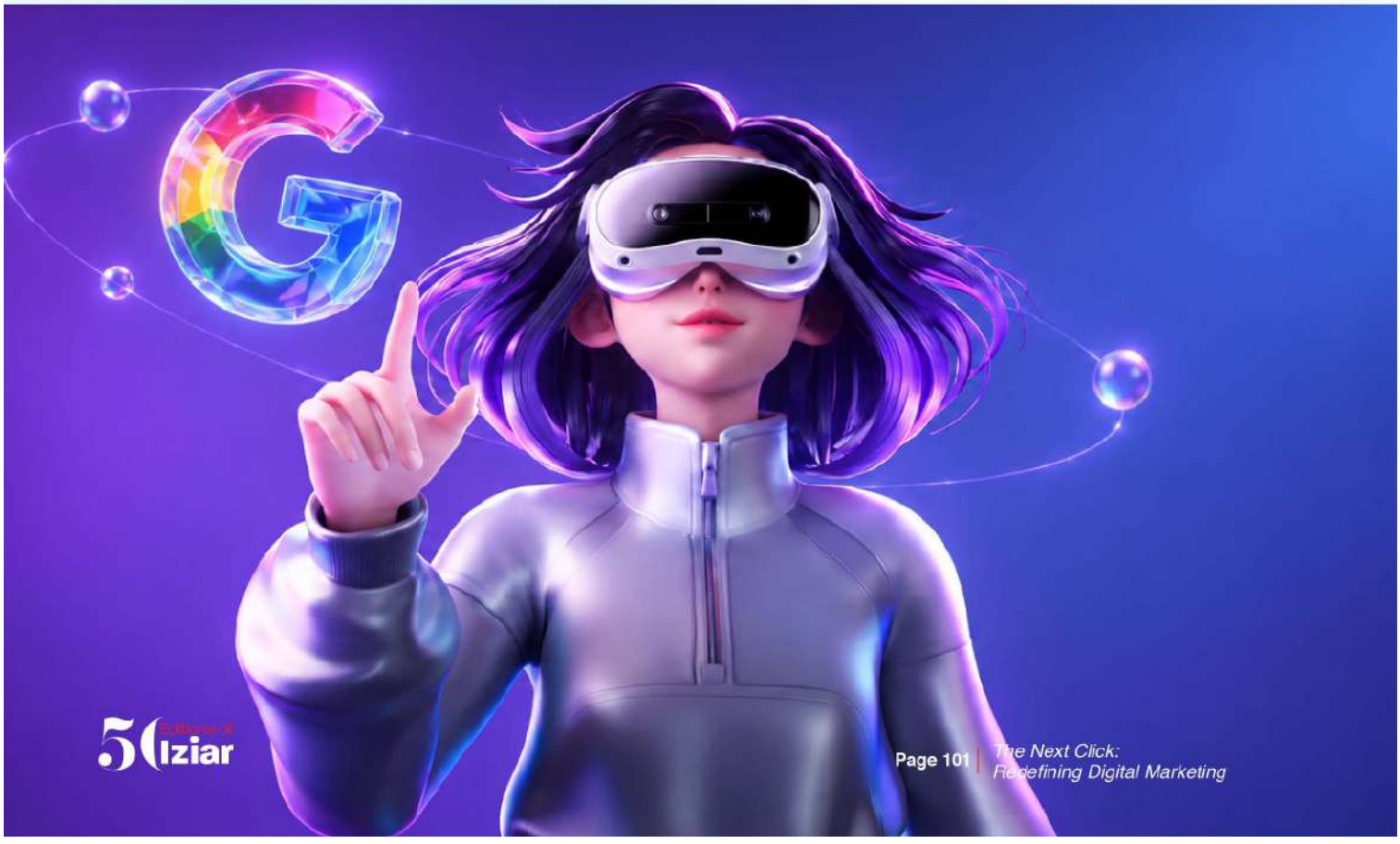
The objective is no longer just to appear on the first page of Google. It is to become a trusted source that both people and AI systems recognise.

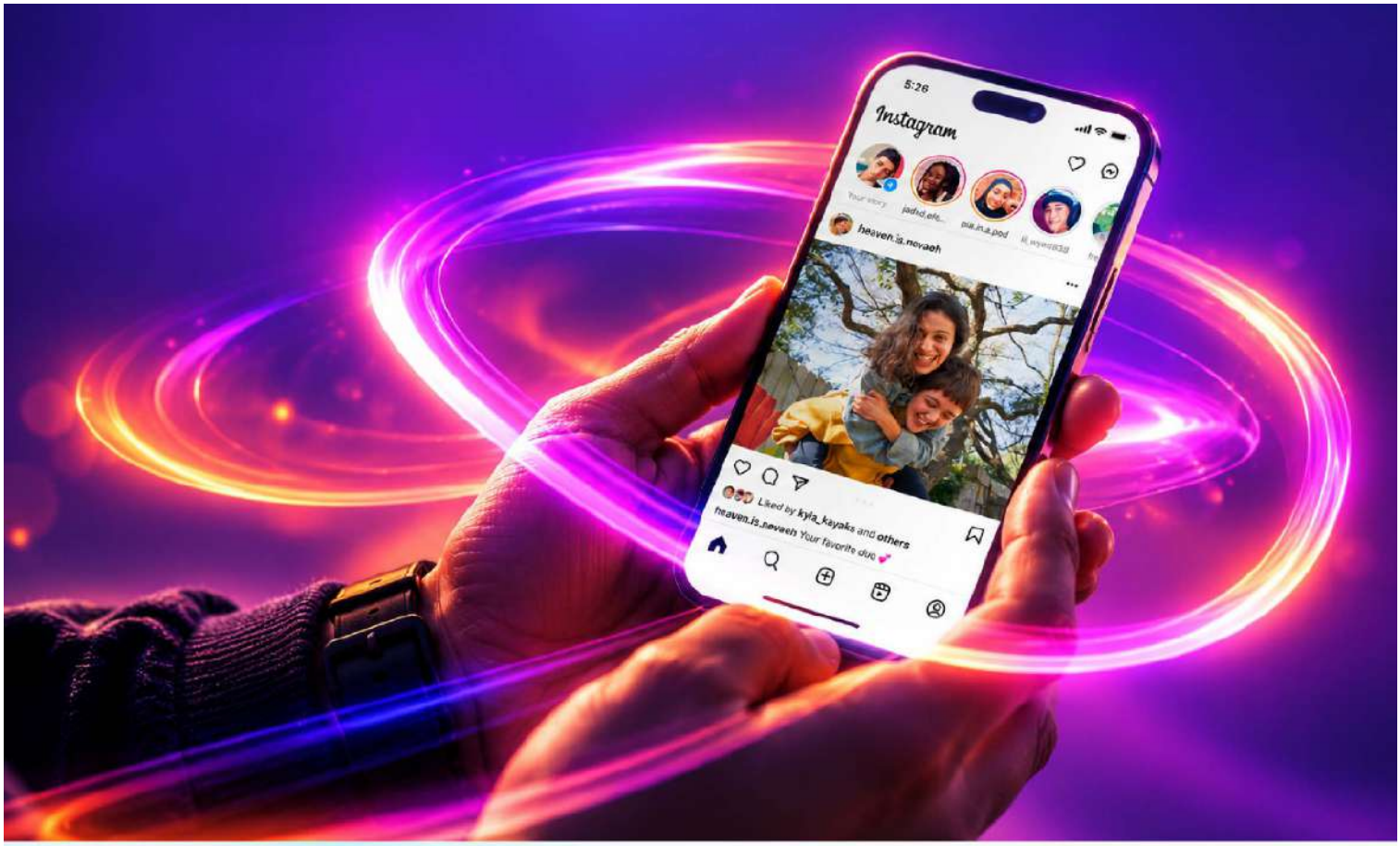
Advertising Is Becoming More Automated

Artificial intelligence is transforming digital advertising by taking over many tasks that once required manual decisions. Tools such as Meta Advantage+ and Google's Performance Max use machine learning to optimise audience selection, bidding, placements, and creative delivery.

These capabilities can help marketers manage campaigns more efficiently. However, automation does not guarantee better results. Performance depends on the quality of the data, the relevance of the advertisements, the campaign objectives, and the accuracy of conversion tracking.

As advertising platforms take on more responsibility, marketers must focus on providing the right inputs. This includes using meaningful conversion data, developing different creative formats, understanding customer behaviour, and setting appropriate budgets and brand-safety controls.





For example, a campaign that generates hundreds of inexpensive enquiries may appear successful. However, if most enquiries fail to become paying customers, the campaign may be wasting money. Feeding qualified leads and actual sales data back into advertising platforms helps direct optimisation towards outcomes that matter. Human judgement remains essential. Marketers should regularly review campaign performance, test automated strategies against reliable benchmarks, and verify whether the results justify the investment.

Measurement Is About More Than Clicks

Accurately measuring digital marketing performance is becoming increasingly difficult. Browser restrictions, consent requirements, and privacy regulations can limit the data available to traditional tracking systems. As a result, some conversions may not be recorded correctly, making campaign performance harder to evaluate.

To address this challenge, businesses are adopting more comprehensive measurement approaches. Server-side tagging, Google's Consent Mode, and Meta's Conversions API can help organisations manage conversion data more effectively when configured appropriately and used in compliance with applicable privacy requirements.

Another important development is the integration of customer relationship management (CRM) systems with advertising platforms. Instead of measuring success only through website visits or form submissions, businesses can use qualified enquiries, completed purchases, and actual revenue to evaluate campaign effectiveness. Incrementality testing provides another useful perspective by helping marketers understand whether an advertising campaign genuinely generated additional sales or simply reached customers who would have purchased anyway.

In India, the Digital Personal Data Protection Act, 2023, and applicable rules and commencement provisions make responsible personal-data handling an important consideration for digital marketers. Clear consent practices, appropriate data use, and transparent processes are becoming essential parts of sustainable marketing.



Conversations Are Becoming the New Conversion Channel

Digital marketing in India is increasingly moving beyond websites and landing pages into messaging platforms. Customers often prefer to ask questions, compare options, check availability, and complete purchases through a conversation rather than navigate a lengthy sales process. Click-to-WhatsApp advertisements, product catalogues, payment links, and automated responses help businesses connect advertising directly with customer conversations. AI-powered assistants can respond to routine enquiries, provide product information, qualify leads, and schedule appointments in different languages.

This approach can reduce friction between discovering a product and taking action. It is particularly useful for businesses where customers need clarification before making a purchase. However, automation must be handled carefully. An assistant that provides incorrect pricing, makes unsupported promises, or shares misleading information can damage customer trust. Businesses should establish clear response guidelines, keep information updated, follow platform policies, and provide a straightforward way for customers to reach a human representative. The strongest approach combines the speed of automation with the judgement and empathy of human support.



The Next Phase: AI Agents and Smarter Commerce

The next stage of digital marketing is moving towards AI agents that can perform multiple tasks with limited supervision. These systems are increasingly being used to analyse campaigns, prepare reports, generate advertising variations, and support marketing workflows. AI-poweredshopping tools are also changing how customers compare products and evaluate purchasing options.

For businesses, these developments create opportunities to improve productivity and personalise customer experiences. However, effective implementation requires accurate data, reliable information, appropriate access controls, and regular human review.

Brands should treat AI as a capable assistant rather than an unquestionable decision-maker. Marketing teams must continue to verify facts, assess creative quality, protect customer information, and ensure that automated decisions align with business objectives. Trust will remain a competitive advantage, even as the technology becomes more sophisticated.



Conclusion: Visibility, Trust, and Measurable Growth

Digital marketing in 2026 is not simply about adopting more tools or following the latest trends. It is about understanding how technology is changing the relationship between businesses and customers.

Search rankings remain valuable, but being referenced by AI systems is becoming another important visibility goal. Automated advertising can improve efficiency, but only when supported by quality data and clear objectives. Advanced tracking can strengthen measurement,

while conversational marketing can make the customer journey faster and more convenient.

Ultimately, successful digital marketing still depends on understanding customer needs, delivering genuine value, and building lasting trust. Businesses that combine human creativity, responsible AI adoption, reliable first-party data, and meaningful performance measurement will be better positioned to turn online visibility into sustainable growth.



AYSHA FIDHA S
CRO, IPCS GLOBAL TRIVANDRUM

The Technologies Building Our Digital Future

The digital world is moving beyond computers that simply follow instructions. Today, machines can analyse information, software can generate content, devices can communicate with one another, and automated systems can perform tasks with minimal human intervention.

These developments are changing how businesses operate, how people interact with technology, and how organizations solve problems. Behind much of this transformation are four key technologies: Artificial Intelligence (AI), Cloud Computing, the Internet of Things (IoT), and Automation.

Each technology has its own strengths. AI helps systems analyze information and make predictions. Cloud computing provides the infrastructure to store data and run applications at scale. IoT connects physical devices to digital systems, while automation turns instructions and decisions into action.

Individually, they offer valuable capabilities. Together, they are creating a more connected, responsive, and intelligent digital ecosystem.

Artificial Intelligence: Giving Technology the Power to Learn

Artificial Intelligence has become one of the most influential forces in modern IT. It enables computer systems to perform tasks associated with human intelligence, including recognizing images, understanding language, identifying patterns, and generating predictions.

Generative AI has expanded these possibilities further. Modern AI tools can assist with writing, software development, design, research, customer support, and data analysis. Tasks that once required considerable time and manual effort can now be completed more quickly with the right tools and human guidance.

Businesses are also using AI to study customer behavior, detect unusual activity, supportdecision-making, and identify opportunities for improvement. In industries such as healthcare, manufacturing, finance, and retail, AI can help professionals make better use of the information available to them.

AI in the Workplace

One of the most important changes is the growing relationship between human workers and intelligent systems. AI can handle certain repetitive tasks, summaries large amounts of information, and assist with technical problem-solving. This gives employees more time to focus on creativity, communication, planning, and decisions that require human judgement.

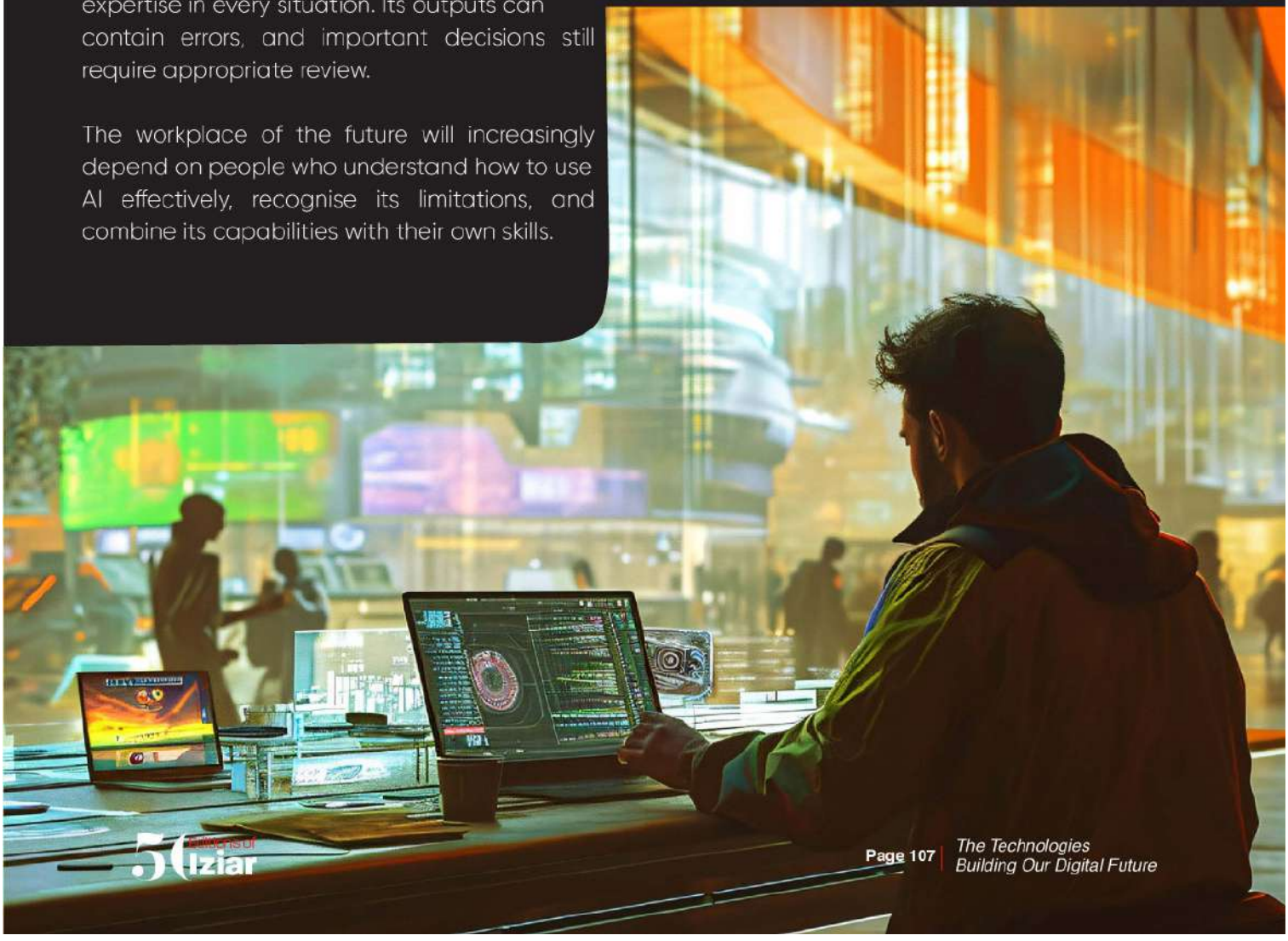
However, AI is not a replacement for human expertise in every situation. Its outputs can contain errors, and important decisions still require appropriate review.

The workplace of the future will increasingly depend on people who understand how to use AI effectively, recognise its limitations, and combine its capabilities with their own skills.

Cloud Computing: The Foundation of a Connected Business

Modern businesses depend on data, applications, and digital services. Managing the entire infrastructure required to support them can be expensive and complex.

Cloud computing offers another approach. Instead of relying entirely on servers and equipment located on their own premises, organizations can access computing power, storage, databases, and software through cloud platforms. Resources can be increased or reduced according to demand, helping businesses respond to changing requirements without building every part of their IT infrastructure from scratch.



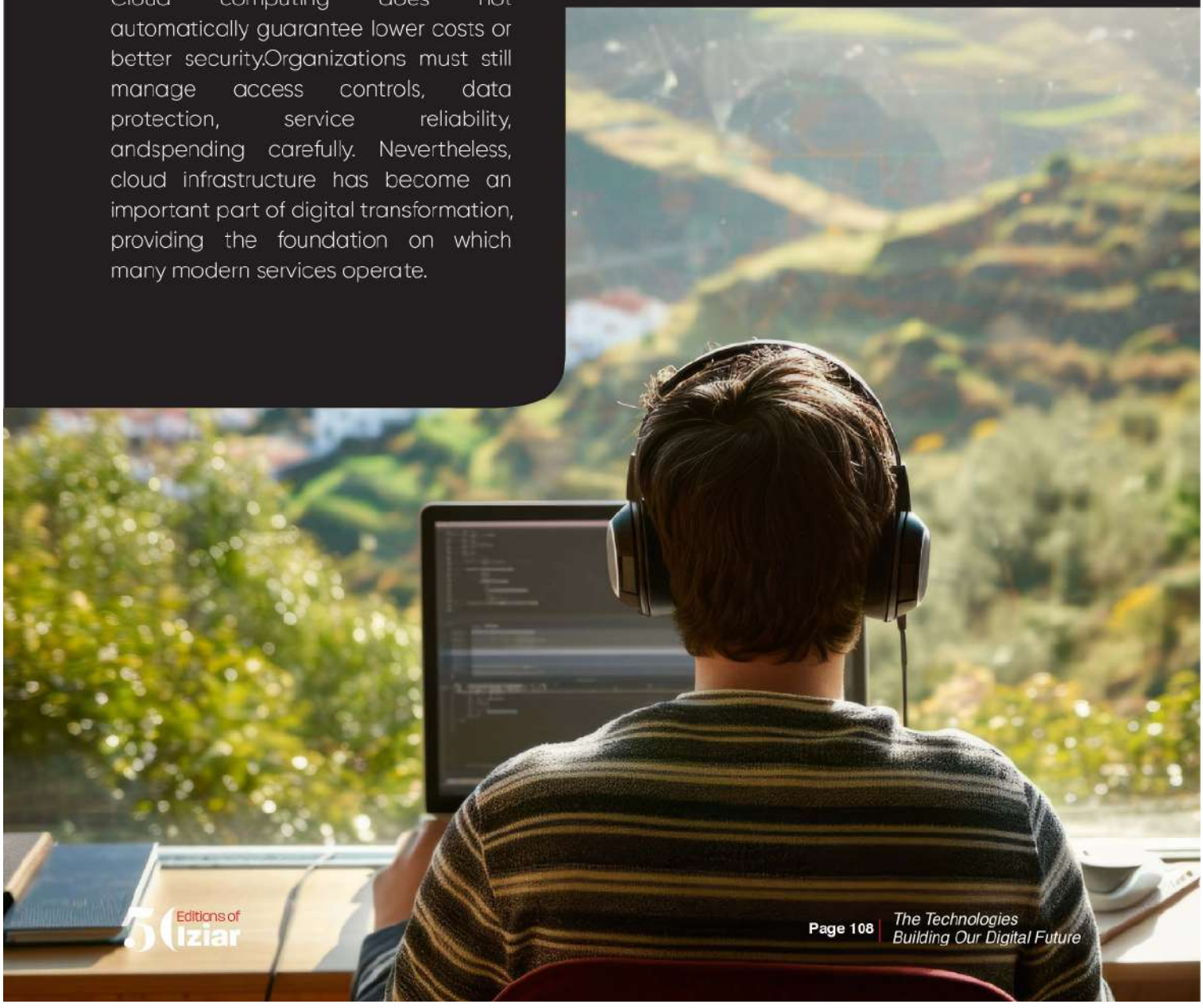
Why Cloud Computing Matters

Cloud technology supports remote working, online services, data storage, software development, AI applications, and connected-device platforms.

Its key advantages include:

Scalability: Resources can grow or shrink as business needs change.
Flexibility: Employees can access supported applications and information from different locations.
Faster deployment: Businesses can launch and update applications without always having to purchase and install physical infrastructure.
Data accessibility: Information can be made available to authorized users across teams and locations.
Support for innovation: Cloud platforms provide computing resources for analytics, AI, and other data-intensive applications.

Cloud computing does not automatically guarantee lower costs or better security.Organizations must still manage access controls, data protection, service reliability, andspending carefully. Nevertheless, cloud infrastructure has become an important part of digital transformation, providing the foundation on which many modern services operate.



Internet of Things: Connecting the Physical and Digital Worlds

The Internet of Things, commonly known as IoT, brings physical devices into the digital world by connecting them to networks that allow them to collect, exchange, and sometimes act on data.
Examples range from smart watches and connected home appliances to industrial sensors, healthcare monitoring equipment, and connected vehicles.

The real value of IoT lies in its ability to provide information about what is happening in the physical world. Instead of relying entirely on manual inspections or occasional measurements, users can monitor conditions continuously or at regular intervals.



IoT in Everyday Life

Imagine a smart home where lights respond to occupancy, heating or cooling adjusts according to settings, and security devices send alerts when unusual activity is detected. In agriculture, sensors can monitor soil moisture and environmental conditions, helping farmers make more informed irrigation decisions. In healthcare, connected devices can record selected measurements and share them with authorised monitoring systems.
Industrial applications are equally significant. Sensors installed on motors, pumps, and other equipment can track factors such as temperature, vibration, and operating conditions.

When the data indicates a developing problem, maintenance teams can investigate before the equipment suffers a major failure.IoT is therefore helping organizations move from occasional observation towards more continuous, data-informed operations.
As connected devices become more widespread, cybersecurity and privacy must remain priorities. An insecure device can become an entry point into a larger network, making secure configuration, software updates, and access management essential.



Automation: Turning Repetitive Work Into Efficient Processes

Automation allows tasks to be completed with less manual intervention. It has long been used in manufacturing and industrial control, but its role now extends across office administration, customer service, software development, marketing, and business operations. Simple automation may involve sending an email when a form is submitted. More advanced systems can coordinate multiple applications, process documents, route customer enquiries, or manage complex workflows.

The objective is not merely to make work faster. Well-designed automation can also improve consistency, reduce avoidable errors, and allow people to focus on tasks that require judgement and problem-solving.

The Rise of Intelligent Automation

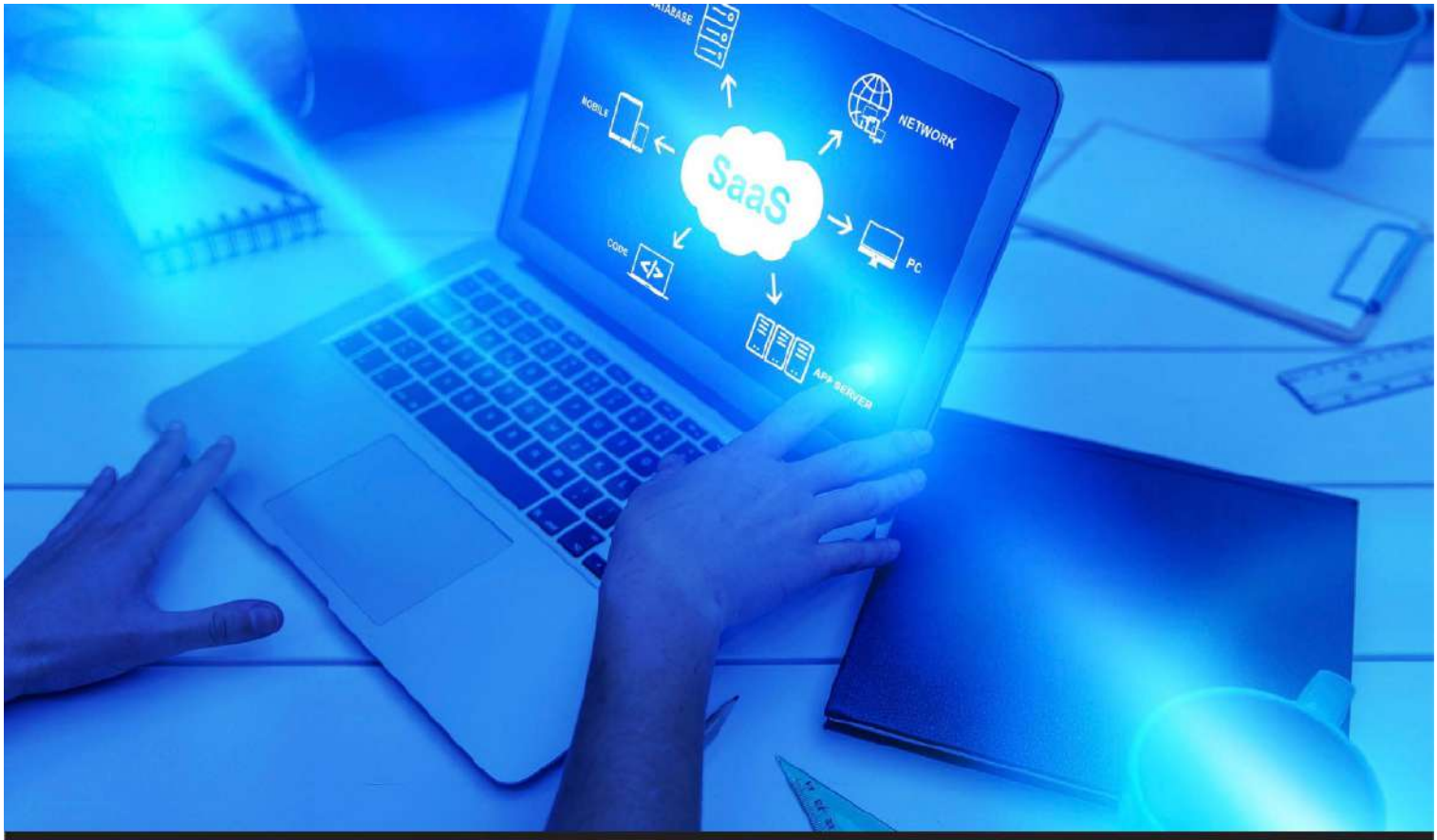
Traditional automation generally follows predefined rules and instructions. Intelligent automation combines automation with technologies such as AI and machine learning to support more adaptive processes.
For example, a conventional system might send every customer enquiry to the same department. An AI-assisted workflow could classify enquiries by subject and urgency before routing them to the appropriate team.

This combination can improve:

- Productivity and operational efficiency.
- Accuracy and consistency in routine tasks.
- Customer service and response times.
- Information processing and decision support.
- Resource utilisation and cost management.

Even advanced automation needs proper supervision. Processes must be tested, exceptions handled, and important decisions reviewed where human oversight is necessary.





When AI, Cloud, IoT, and Automation Work Together

The most significant changes often happen when these technologies are combined rather than used independently.
Consider a modern manufacturing plant.

Sensors attached to production equipment collect information about temperature, vibration, and operating performance. An IoT network transfers this data to a system where it can be stored and processed. Cloud infrastructure provides the computing resources needed to manage large volumes of information, while AI analyses patterns and estimates the likelihood of equipment failure.
When the system identifies a potential problem, automation can generate an alert, create a maintenance request, or notify the responsible engineer. Depending on the application and its safety requirements, it may also initiate an approved control action.

Instead of waiting for a machine to fail, the maintenance team can investigate the warning and take appropriate action.

The same principle can be applied to energy management, logistics, smart buildings, agriculture, and many other fields.
The process can be summarized as:

CONNECT → COLLECT → ANALYSE → PREDICT → ACT

IoT connects devices and gathers information. Cloud infrastructure supports storage and processing. AI helps identify patterns and make predictions. Automation turns the resulting decisions into action.
This integration is helping businesses build systems that are more responsive and data-driven.
Its effectiveness, however, depends on reliable data, suitable infrastructure, secure connections, and well-designed processes.

The Challenges behind the Digital Transformation

The growing use of intelligent and connected technologies creates opportunities, but it also introduces risks that organizations cannot afford to ignore.

Cybersecurity becomes more complex as businesses connect additional devices,applications, and networks. Each new connection must be protected against unauthorized access and misuse.

Data privacy is another major concern. AI and analytics systems may process large amounts of personal or commercially sensitive information, making responsible collection, storage, and use essential.

Reliability and accuracy also matter. Incorrect data or flawed AI predictions can lead to poor decisions, while failures in automated systems can interrupt operations.

There are also questions about employment, accountability, algorithmic bias, and the responsible use of emerging technologies. Automation may change the tasks people perform, creating a greater need for reskilling and new professional capabilities. Organizations must therefore approach digital transformation as more than a technology upgrade. It also requires sound governance, employee training, risk management, and a clear understanding of the problems each technology is intended to solve.



The IT Professional of Tomorrow

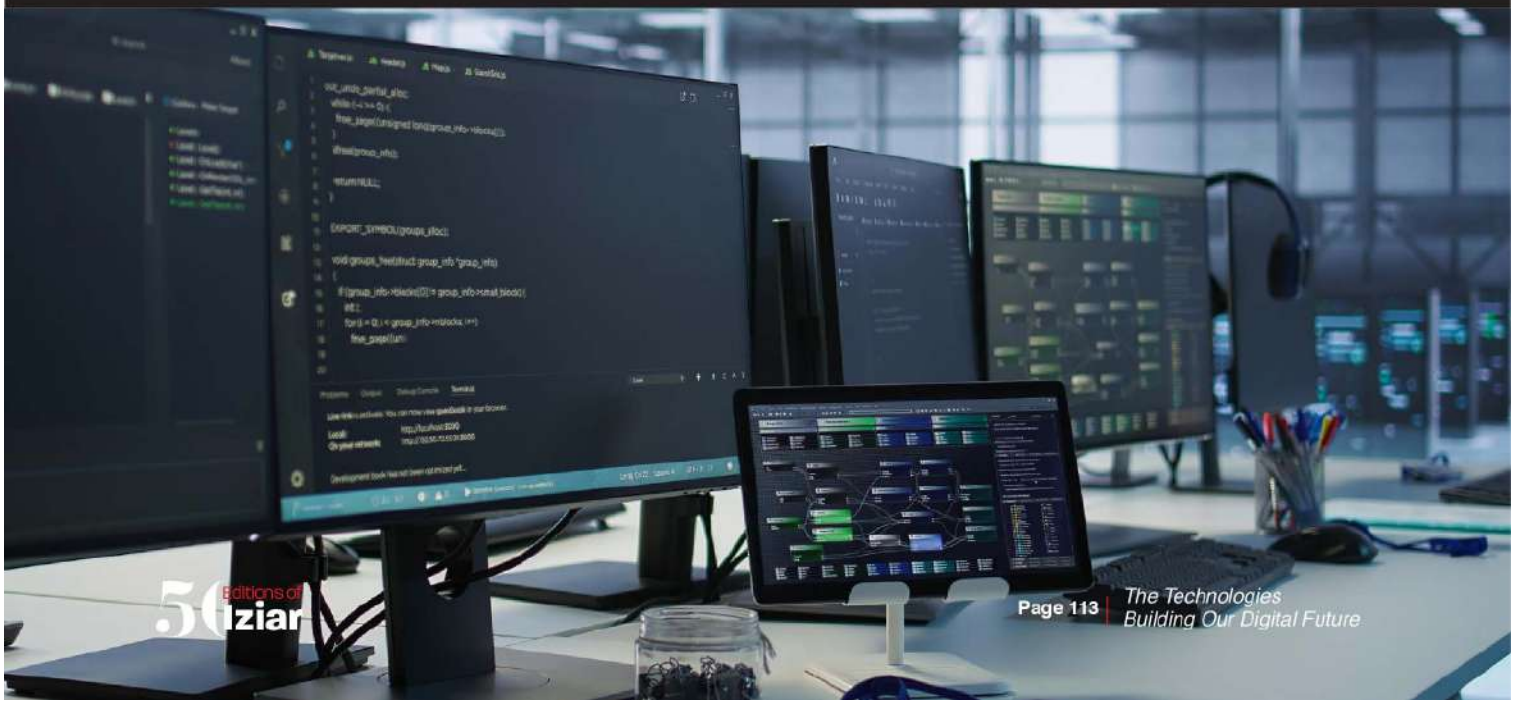
As technology evolves, so do the skills required to work with it. Technical knowledge remains important, but professionals must also be willing to adapt, collaborate, and learn throughout their careers. Several fields are likely to remain important across the evolving IT landscape:

- Artificial Intelligence and Machine Learning.
- Cloud Computing and Cloud Engineering.
- Cybersecurity and Information Security.
- Data Science and Business Analytics.
- IoT and Embedded Systems.
- Automation, Robotics, and Industrial Control.
- Software Development and Application Engineering.
- DevOps and Site Reliability Engineering.
- AI-enabled Business Transformation.



These fields increasingly overlap. A developer may need to understand cloud deployment, an automation engineer may work with industrial data analytics, and a cybersecurity specialist may need to assess connected devices and AI-powered systems.
For students, building a strong foundation in programming, networking, databases, and problem-solving can provide a valuable starting point. Practical projects, internships, certifications where appropriate and continuous learning can help turn that foundation into professional capability.

For experienced professionals, updating existing skills and understanding how emerging technologies fit into their field can open new opportunities.
The advantage will not necessarily belong to those who know the greatest number of tools. It will belong to those who understand how to apply technology to real problems.



Looking Ahead: One Digital Ecosystem

The future of IT will not be defined by a single technology replacing everything that came before it. It will be shaped by technologies working together to create solutions that are more useful, connected, and adaptable.

AI will help systems interpret information and generate insights. Cloud computing will provide scalable infrastructure. IoT will connect physical equipment and environments to digital platforms. Automation will help turn information and decisions into practical action.

Together, these technologies are changing how organizations manage information, deliver services, maintain equipment, and make decisions.





The Future Is Already Taking Shape

The transformation of the digital world is not a distant possibility. It is already visible in the applications we use, the devices around us, and the systems businesses rely on every day. Yet technology alone does not guarantee progress. Its real value depends on how thoughtfully it is designed, how responsibly it is used, and how effectively people adapt to it. For students, this is an opportunity to develop skills that will remain relevant as the industry changes. For professionals and organizations, it is a reminder that continuous learning and responsible innovation are essential.

The question is no longer whether AI, Cloud, IoT, and Automation will influence the future of IT. It is how we will combine these technologies to build a smarter, safer, and more useful digital world.

Fifty Editions, One Vision:

Celebrating the Journey of Iziar

In September 2022, we embarked on a meaningful journey with the launch of the very first edition of Iziar—a magazine envisioned as a platform to share knowledge, showcase talent, celebrate achievements, and inspire continuous learning. Today, as we proudly present the 50th edition, we celebrate not merely a publishing milestone but a remarkable journey built on vision, dedication, creativity, and collective effort. Reaching fifty editions is a testamate to the power of shared ideas and the commitment of everyone who has contributed to the growth of Iziar.



From its humble beginnings to this golden milestone, the magazine has evolved into a platform that brings together technical expertise,industry insights, professional experiences, and organizational achievements. On this special occasion, the editorial team extends its heartfelt gratitude to everyone who has made this journey possible.

Anand Sai
Editor-in-Chief

First and foremost, we express our deepest gratitude to our esteemed **Board of Directors, Mr. Ubaidulla Mekkuth and Mr. Jamal Nadakkavil,** whose vision, valuable ideas, and constant motivation have been instrumental in shaping Iziar. Their encouragement and belief in the power of knowledge-sharing have inspired us to explore new possibilities, raise our standards, and make every edition more meaningful. Their vision has been the driving force behind this initiative, and the 50th edition stands as a proud reflection of their continued support and encouragement.

We extend our sincere appreciation to Mr. Ajith Surendran, General Manager, and Mr. Rakesh K. C, Technical Head, for their guidance, leadership, and unwavering support throughout this journey. Their encouragement has helped us bring together valuable technical knowledge and organizational accomplishments, making Iziar a platform for learning and inspiration. We also convey our heartfelt thanks to the HR team for their cooperation, coordination, and support in bringing people, ideas, and contributions together. Our gratitude also goes to the Territory Managers, Branch Managers, and Sales Team members for their valuable coordination, encouragement, and efforts in promoting participation and gathering contributions from across the organization.

We sincerely acknowledge the Regional Technical Heads, Territory Technical Heads, and all technical team members across our branches, whose expertise, practical experience, innovative thinking, and enthusiasm for sharing knowledge have enriched the magazine and strengthened its technical value.



We also extend our appreciation to the Placement Team for their valuable contributions in highlighting career opportunities, student achievements, industry connections, and professional development. Their efforts help reinforce the importance of employability, practical skills, and industry readiness, adding another meaningful dimension to Iziar.

A special note of appreciation goes to the Design team, whose creativity, artistic vision, and meticulous attention to detail have given Iziar its distinctive identity. Their wonderful designs and dedicated efforts have transformed articles and ideas into an engaging and visually appealing publication. Their contribution has played an essential role in making every edition a magazine to be proud of.

Above all, we thank every contributor, writer, reviewer, and well-wisher who has supported Iziar over the years. Every article submitted, idea shared, suggestion offered, and effort made has contributed to this achievement. This milestone belongs to everyone who has been part of the journey, whether through a single contribution or sustained support across multiple editions. As we celebrate fifty editions, we look back with pride and forward with renewed enthusiasm. We aspire to make Iziar an even stronger platform for knowledge, innovation, creativity, and collaboration—one that continues to inspire our people, celebrates our achievements, and connects us through the power of shared learning.

From The First Edition In September 2022 To This Landmark 50th Edition

Every step has been made possible by a shared vision and collective commitment. Fifty editions later, our purpose remains unchanged: to learn, to share, and to grow together. Thank you for being an integral part of the Iziar journey. This milestone is not the achievement of one team or one individual—it is a celebration of all of us.

With sincere appreciation and warm regards,

The Editorial Team

Become a Part of World's Trusted Industry-Based Training Provider

Ai - Digital Marketing

Industrial Automation

Python & Data Science

Embedded & IoT

Smart Home Automation

Artificial Intelligence

Cybersecurity and Ethical Hacking

+91 9846 770 771 | INDIA | QATAR | DUBAI | SAUDI ARABIA